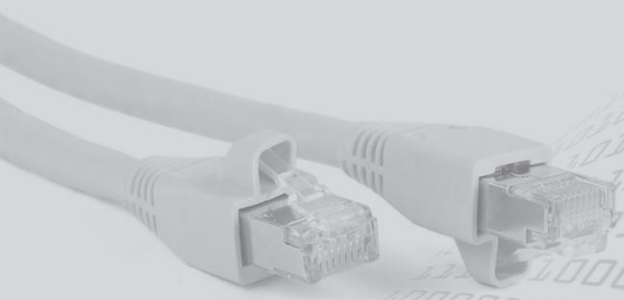
ТЕЛЕКОММУНИКАЦИИ: СЕТИ И ТЕХНОЛОГИИ,

АЛГЕБРАИЧЕСКОЕ КОДИРОВАНИЕ И БЕЗОПАСНОСТЬ ДАННЫХ

МАТЕРИАЛЫ МЕЖДУНАРОДНОГО НАУЧНО-ТЕХНИЧЕСКОГО СЕМИНАРА

(Минск, январь–декабрь 2012 г.)



Министерство образования Республики Беларусь
Учреждение образования
«Белорусский государственный университет информатики
и радиоэлектроники»

ТЕЛЕКОММУНИКАЦИИ: СЕТИ И ТЕХНОЛОГИИ, АЛГЕБРАИЧЕСКОЕ КОДИРОВАНИЕ И БЕЗОПАСНОСТЬ ДАННЫХ

МАТЕРИАЛЫ МЕЖДУНАРОДНОГО НАУЧНО-ТЕХНИЧЕСКОГО СЕМИНАРА

(Минск, январь – декабрь 2012 г.)

TELECOMMUNICATIONS: NETWORKS AND TECHNOLOGIES, ALGEBRAIC CODING AND DATA SECURITY

Минск БГУИР 2012

УДК 621.391:004.056.55
ББК 32.811+32.973.26-018.2
Т31

Телекоммуникации: сети и технологии, алгебраическое
Т31 кодирование и безопасность данных : материалы международного научно-технического семинара (Минск, январь – декабрь 2012 г.) = Telecommunications: Networks and Technologies, Algebraic Coding and Data Security – Минск : БГУИР, 2012. – 88 с.
ISBN 978-985-488-939-9.

Сборник содержит статьи по телекоммуникациям: сетям телекоммуникаций и информационной безопасности в области научно-теоретических разработок и прикладных применений, алгебраическому кодированию и обработке изображений, программно-аппаратным и защитным средствам обеспечения в телекоммуникационных сетях.

Для научных сотрудников в области телекоммуникаций, преподавателей, аспирантов, магистрантов и студентов технических вузов.

Научное издание

Корректор *Т. В. Мироненко*
Ответственный за выпуск *В. К. Конопелько*
Компьютерный дизайн и верстка *Е. Г. Макейчик*

Подписано в печать 10.12.2012. Формат 60×84 ⅛. Бумага офсетная. Гарнитура «Таймс».
Отпечатано на ризографе. Усл. печ. л. 10,46. Уч.-изд. л. 8,9. Тираж 50 экз. Заказ 678.

Издатель и полиграфическое исполнение: учреждение образования
«Белорусский государственный университет информатики и радиоэлектроники»
ЛИ №02330/0494371 от 16.03.2009. ЛП №02330/0494175 от 03.04.2009.
220013, Минск, П. Бровки, 6

ISBN 978-985-488-939-9

СОДЕРЖАНИЕ

CONTENTS

ТЕЛЕКОММУНИКАЦИИ: СЕТИ И ТЕХНОЛОГИИ, АЛГЕБРАИЧЕСКОЕ КОДИРОВАНИЕ И БЕЗОПАСНОСТЬ ДАННЫХ

УДК 004.932.2

КОДИРОВАНИЕ ПАНОРАМНЫХ ВИДЕОДАННЫХ, УПРАВЛЯЕМОЕ ОПЕРАТОРОМ

К.А. ВОЛКОВ, В.Ю. ЦВЕТКОВ

Белорусский государственный университет информатики и радиоэлектроники
П. Бровки, 6, Минск, 220013, Беларусь

Поступила в редакцию 2 октября 2012

В статье проводится анализ основных способов сжатия панорамных видеоданных для передачи в мобильных сетях. Предлагается метод сжатия панорамных видеоданных, использующий управляющую связь от оператора.

Ключевые слова: панорамные видеоданные, сжатие видео, мобильные сети.

Введение

Системы видеонаблюдения находят широкое применение в образовании, медицине, промышленности, безопасности и т.д. С удешевлением оборудования и совершенствованием технологий съемки, обработки, передачи и хранения мультимедийных данных возможным становится использование панорамного видеонаблюдения, в том числе и в мобильных сетях. Однако из-за естественного ограничения на скорость передачи и значительного размера данного типа информации актуальной становится задача сжатия.

Большой эффективности в сокращении избыточности панорамных видеоданных можно достичь за счет использования двух подходов: устранения временной и пространственной избыточности видеоданных и удаления незначимой информации с учетом психовизуальных особенностей человеческого восприятия изображений. Оба способа относятся к классу сжатия с частичной потерей информации, т.е. не ставят перед собой цель абсолютно точного и полного восстановления исходных видеосигналов, а предназначены для максимального сжатия видеосигнала при минимальных субъективных искажениях восстанавливаемого сигнала. Первый подход достаточно хорошо проработан и имеет реализации в виде промышленных алгоритмов видеокодеков [1-3], учитывающих внутрикадровую (MJPEG, MJPEG 2000), межкадровую (CinePack) и оба типа избыточности (MPEG-1,2,4, H.264). Видеокодеки различаются по вычислительной сложности алгоритмов и коэффициенту сжатия видеоданных, однако для них характерны рост вычислительных затрат и размер сжатых видеоданных практически пропорционально разрешению видео (табл. 1). Это делает затруднительным их непосредственное применение для передачи панорамных видеоданных в мобильных сетях.

Таблица 1. **Требуемая пропускная способность каналов передачи данных (Мбит/сек) для видео различного разрешения**

Разрешение	MJPEG	MPEG-4	H.264
320×240	1,3	0,5	0,3
384×288	1,8	0,7	0,4
640×480	5	1,9	1
768×576	7	2,7	1,6
1024×768	13	5	2,8
1920×1080	34	13	7,5

Второй подход реализуется за счет использования подвижных поворотных видеокамер с дистанционным управлением и аппаратных детекторов движения [4, 5]. Недостатками данных методов являются необходимость использования подвижных механизмов, имеющих значительное время реакции, энергопотребление.

Из анализа задач оператора панорамного видеонаблюдения следует, что требуется осуществлять непосредственное наблюдение за пространством в поле зрения и получать информацию об изменении обстановки вне поля зрения (появлении подвижных площадных объектов внутри контролируемого периметра). Целью данной работы является разработка метода кодирования панорамных видеоданных в мобильной сети с оператором.

Метод сжатия панорамных видеоданных

Предлагается метод селективного кодирования панорамных изображений в мобильных сетях с оператором, основанный на использовании при кодировании видеоданных информации о секторе наблюдения оператора. Сущность метода состоит в формировании изображения, состоящего из фрагмента панорамного изображения в поле зрения оператора и пиктографической информации о подвижных объектах вне поля зрения. Метод позволяет снизить размер кодированного изображения за счет селективного исключения информации о неподвижных объектах вне поля зрения оператора. Метод включает в себя следующие основные шаги:

1) формирование кругового панорамного изображения;

2) определение направления взгляда оператора;

3) определение подвижных объектов на панорамном изображении;

4) определение относительных координат подвижных объектов в пространстве;

5) выделение фрагмента панорамного изображения в поле зрения оператора;

6) формирование пиктографических изображений для подвижных объектов вне поля зрения оператора;

7) формирование изображения, включающего фрагмент панорамного изображения в поле зрения оператора и пиктографические изображения подвижных объектов.

Предлагаемый в статье метод может быть применен для работы оператора в нашлемной системе индикации или очках виртуальной реальности с использованием системы определения направления взгляда. В таком случае поле зрения оператора, составляющее 60-120 градусов, в пределах которого он способен эффективно воспринимать информацию [6], является психовизуальной особенностью, за счет которой возможно осуществить дополнительное сжатие видео.

Анализ обобщенной модели канала [7, 8] для задачи кодирования панорамных видеоизображений (см. рис. 1) показывает, что задача селективного кодирования может решаться за счет модификации кодера первичного кода. Соответственно, при этом не требуется модификация кодера источника и криптографического кодера, так что возможно использование для них существующих стандартных программных и аппаратных решений.

Для модификации кодера первичного кода для снижения разрешения с целью уменьшения размера исходного панорамного изображения предлагается модификация модели канала с добавлением управляющей связи для кодера первичного кода. Схема преобразования видеоданных, обеспечивающая селективное кодирование информации, представлена на рис. 2.

Такой подход имеет следующие преимущества:

- возможность использования существующих программных и аппаратных кодеров источника;
- снижение размера исходных данных для кодера источника и, как следствие, снижение требований к его быстродействию и увеличение энергоэффективности кодирующего оборудования мобильной сети;
- снижение размера выходных данных кодера источника и, как следствие, снижение объема передаваемой по сети информации;
- предварительное ранжирование информации по степени важности для оператора и, как следствие, снижение нагрузки на оператора и уменьшение количества человеческих ошибок.

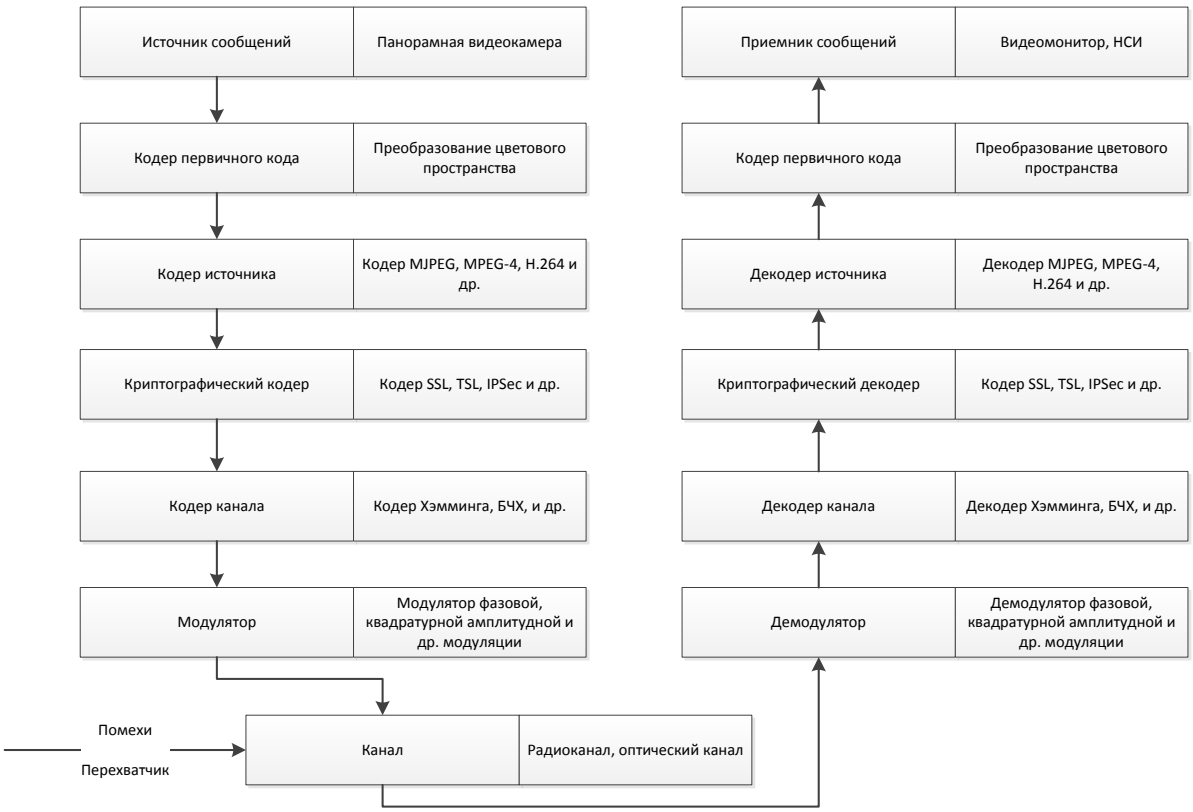


Рис. 1. Обобщенная модель канала передачи панорамных видеоданных

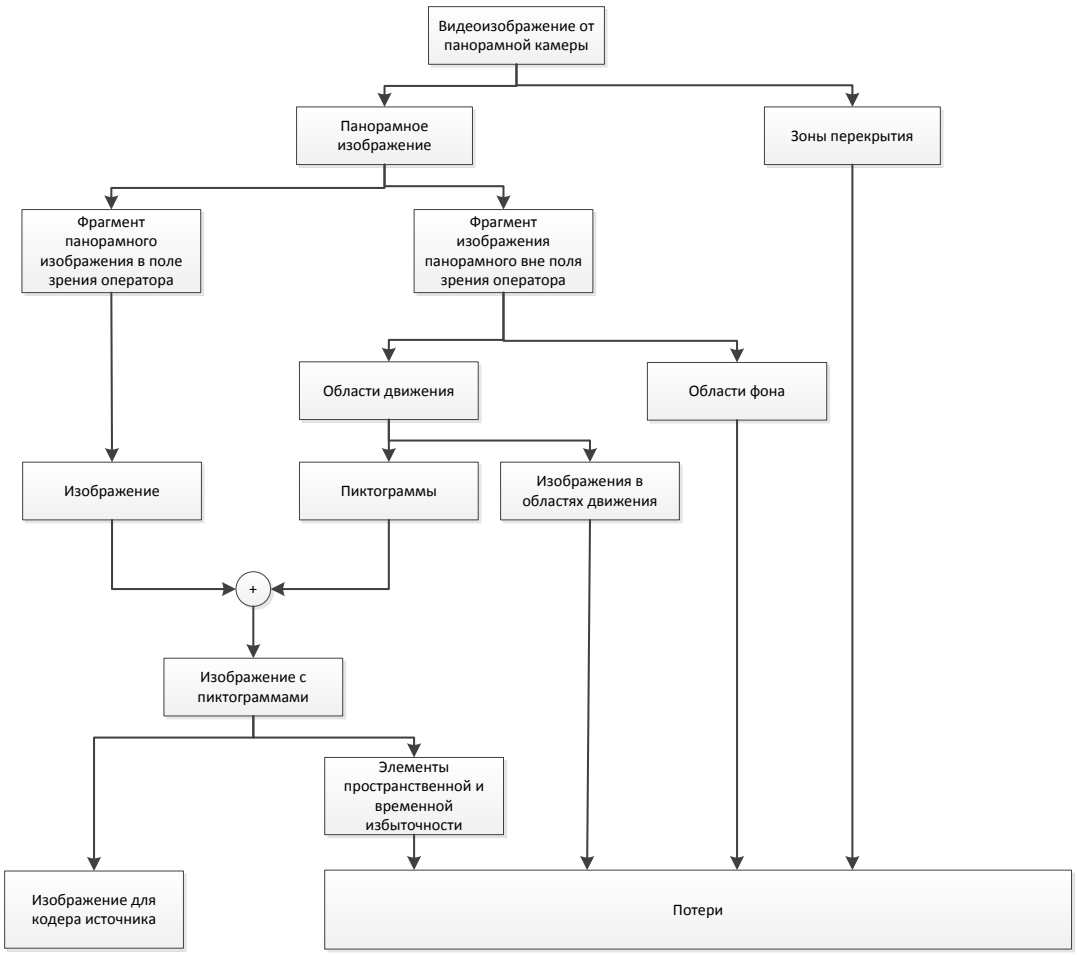


Рис. 2. Селективное кодирование панорамных видеоданных

Для формирования управляющей связи с кодером первичного кода используется информация от системы определения направления взгляда оператора [5, 9], содержащая данные об углах поворота головы в трех плоскостях.

Предлагается следующая модель первичного кодера с потерями, дифференцирующего изображение источника на изображения для кодера источника и теряемую информацию (рис. 3).

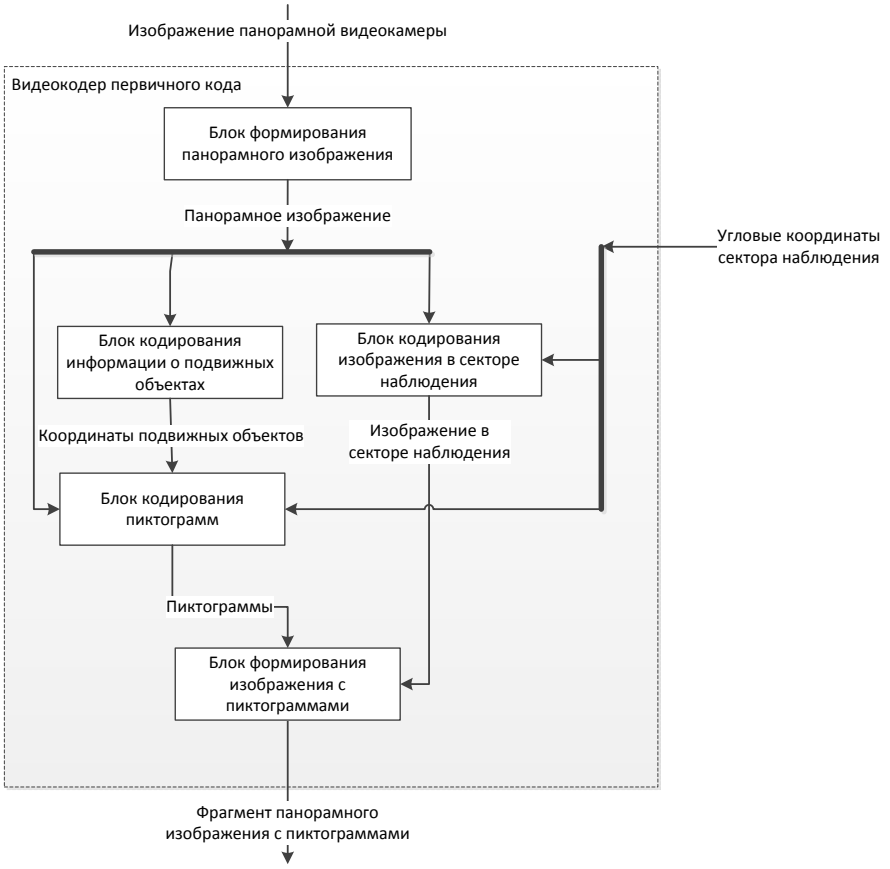


Рис. 3. Кодер первичного кода панорамных видеоданных.

С учетом предложенной модели, кодер первичного кода должен решать следующие задачи:

- формирование кругового панорамного изображения (сшивка) с учетом областей пространственного перекрытия кадров [4, 10];
- выделение фрагмента панорамного изображения, расположенного в поле зрения оператора;
- снижение разрешения изображения в периферической зоне поля зрения оператора;
- выделение подвижных объектов на панорамном изображении [11];
- определение координат (угловых или пространственных) для выделенных объектов;
- совмещение информации о подвижных объектах (пиктограмм) и изображения в поле зрения оператора [10].

Предлагается модель кодера первичного кода, отвечающая вышеизложенным требованиям. На вход кодера поступает информация с обеспечивающих круговой обзор 6 цветных RGB видеокамер, каждая из которых обладает разрешением 768×576 пикселей и имеет площадь области перекрытия кадров 5%. Информация о направлении взгляда оператора составляет 6 байт.

На выходе кодера формируется цветное RGB изображение с разрешением 768×576 пикселей.

Модель видеокодека

Модель состоит из следующих блоков: блока формирования панорамного изображения, блока кодирования изображения в секторе наблюдения, блока кодирования пиктограмм и блока формирования изображения с пиктограммами. На вход блока формирования панорамного изображения, являющегося входом кодера, поступает информация от видеокамер. На выходе блока формируется сшитое панорамное изображение, не содержащее областей перекрытия. Блок кодирования информации в секторе наблюдения выделяет из сформированного кругового панорамного изображения фрагмент, соответствующий направлению взгляда оператора. Блок кодирования информации о подвижных объектах выделяет на панорамном изображении площадные подвижные объекты и определяет их угловые или трехмерные координаты относительно панорамной видеокамеры. Блок кодирования пиктограмм с учетом информации о координатах сектора наблюдения, координатах подвижных объектов и произвольной дополнительной мультимедийной информации формирует пиктограммы с текстовым и графическим представлением данных. Блок формирования изображения с пиктограммами совмещает фрагмент панорамного изображения и пиктографическую информацию и подает на выход кодера.

Таким образом, блок предварительного кодирования теоретически обеспечивает сжатие информации с 6×768×576×3 байт до 768×576×3 байт, что соответствует сжатию на 83%.

Результаты испытания

Произведен натурный эксперимент для определения быстродействия отдельных программных блоков. В эксперименте тестирования кодера и декодера использовались идентичные компьютеры со следующей конфигурацией: чипсет Zotac IONITX-G-E Nvidia ION, процессор Intel Atom N330 dual-core 1,6 GHz, ОЗУ 2xDDR2-800 1 Гб. Время обработки одного кадра программными блоками видеокодека приведено в табл. 2. Требования к пропускной способности сети при использовании в качестве кодера источника метода MJPEG приведены в табл. 3.

Таблица 2. **Время обработки одного кадра программными блоками видеокодека**

Программный блок	Время обработки, мс
Блок выделения областей с движущимися объектами	10
Блок синтеза видеоизображения (с наложением пиктограмм)	2
Блок кодирования видеоизображения	22
Блок декодирования видеоизображения	8
Блок определения положения головы оператора	12

Таблица 3. **Требования к пропускной способности мобильной сети**

Размер изображения	Обеспечиваемый коэффициент сжатия видеоданных	Требуемая скорость канала передачи, Мбит/сек
Полноразмерное панорамное изображение 768×576×6, 25 кадров/сек	1	45
Изображение для использование в НСИ 768×576, 25 кадров/сек	6	8
Изображение для использование в НСИ 640×480, 25 кадров/сек	9	5

Анализ данных табл. 2 показывает, что время обработки одного видеокадра кодером не превышает 34 мс, т.е. система может работать в режиме реального времени для видеопотока с частотой 25 кадров/с. Данные практической оценки требуемой пропускной способности мобильной сети, приведенные в табл. 2, подтверждают теоретическую оценку коэффициента сжатия данных.

Заключение

Предложен метод эффективного кодирования панорамных видеоданных, основанный на использовании информации о секторе наблюдения оператора. Предложенный метод позволяет достичь значительного сжатия видеоданных за счет устранения информации, которая не

может быть воспринята оператором, компактного пиктографического представления данных о подвижных объектах вне поля зрения, устранения пространственной и временной избыточности. Установлено, что предложенный метод позволяет увеличить коэффициент сжатия видеоданных в 6 и более раз по сравнению с методами, не учитывающими особенности функционирования оператора.

PANORAMIC VIDEO CODING CONTROLLED BY THE OPERATOR

K.A. VOLKOV, V.Yu. TSVIATKOU

Abstract

The main methods of panoramic video compression for transmission in mobile networks are analyzed. A method of compression of panoramic video, which uses the control connection to the operator, is proposed.

Литература

1. *Прэтт У.* Цифровая обработка изображений. М., 1982.
2. *Миано Дж.* Форматы и алгоритмы сжатия изображений в действии. М., 2003.
3. *Арюшенко В.М., Шелухин О.И., Афонин М.Ю.* Цифровое сжатие видеоинформации и звука. М., 2003.
4. *Волков К.А., Конопелько В.К.* // 5-я Международная научная конференция по военно-техническим проблемам, проблемам обороны и безопасности, использованию технологий двойного применения MILEX-2011. 25-26 мая 2011. С. 101-103.
5. *Кучерявый А.А.* Бортовые информационные системы. Ульяновск, 2004.
6. *Волков К.А., Конопелько В.К.* // Докл. БГУИР. 2012. №4. С. 12-16.
7. *Конопелько В.К., Липнинский В.А., Дворников В.Д. и др*. Теория прикладного кодирования. Минск, 2004.
8. *Жданов О.Н., Золотарев В.В.* Методы и средства криптографической защиты информации. Красноярск, 2007.
9. *Волков К.А.* // Телекоммуникации: сети и технологии, алгебраическое кодирование и безопасность данных: материалы международного научно-технического семинара. Минск, 2011. С. 33-39.
10. *Волков К.А., Сиротко И.И.* // Телекоммуникации: сети и технологии, алгебраическое кодирование и безопасность данных: материалы международного научно-технического семинара. Минск, 2011. С 57-61.
11. *Волков К.А.* // Докл. БГУИР. 2012. №1. С. 92-98.

УДК 621.391

МОДЕЛИРОВАНИЕ ДВИЖЕНИЯ УЗЛОВ ЛОКАЛЬНОЙ МОБИЛЬНОЙ СЕТИ НА ОСНОВЕ ДИНАМИЧЕСКОГО ХАОСА

А.А. ПОДЛУЦКИЙ, В.Ю. ЦВЕТКОВ, К.Т.Х. АЛЬ-ШАМАРИ

Белорусский государственный университет информатики и радиоэлектроники
П. Бровки, 6, Минск, 220013, Беларусь

Поступила в редакцию 22 октября 2012

Предложен метод пространственно-временной хаотической параметризации движения точек в двухмерном пространстве на основе клеточных автоматов для построения модели мобильности локальной сети с хаотическим движением узлов. Метод обеспечивает хаотическое изменение параметров движения для произвольного числа узлов локальной мобильной сети за счет определения пространственно-временной хаотической динамики во всех точках пространства. Показано, что для снижения вычислительной сложности пространственно-временной хаотической параметризации движения может быть использовано фрактальное расширение хаотического пространства с помощью рекурсивных перестановок.

Ключевые слова: локальные мобильные сети, модели мобильности, динамический хаос.

Введение

В условиях интенсивного развития сетецентрических технологий исследование протоколов локальных мобильных сетей является актуальной задачей. Одной из основных проблем проведения исследований в данном направлении является высокая стоимость экспериментов, связанная с необходимостью использования большого числа узлов, рассредоточенных на значительной площади; выделения значительного времени и частотных ресурсов; создания внешних условий работы сети, таких как естественные и искусственные помехи, погодные условия. Решение данной проблемы возможно за счет использования программных моделей мобильности. Для определения траекторий перемещения узлов локальных мобильных сетей могут быть использованы модели двух типов: натуральные и искусственные [1]. Натуральные модели строятся на основании наблюдений за перемещением объектов в реальных условиях. Такие модели предоставляют точную информацию о реальном местоположении объектов в любой момент времени. Однако их построение также связано с существенными материальными и временными затратами, особенно, при наблюдении большого числа узлов. Искусственные модели позволяют решить данную проблему. Известные искусственные модели мобильности можно разделить на два класса: модели с независимым и групповым движением узлов [2]. Данные модели отличаются низкой сложностью построения, однако они не учитывают пространственно-временную хаотическую динамику параметров движения узлов, проявляющуюся в реальных условиях. Модели мобильности с хаотическим движением узлов в настоящее время не исследованы. Для их построения необходимо формирование хаотического пространства, состояние каждой точки в котором зависит от состояний соседних точек. Известны методы формирования пространственного динамического хаоса, основанные на системах уравнений Лоренца, Рёсслера, Ван дер Поля; отображениях Хенона, Икеды, логистическом; функциях Вейерштрасса-Мандельброта, Мэки-Гласса и ряд других [3]. Однако непосредственное применение этих методов для формирования пространственно-временной хаотической динамики неэффективно. Кроме того, данные методы имеют высокую вычислительную сложность. Единственной моделью пространственно-временного динамического хаоса является клеточный автомат [4]. Его важным достоинством является низкая вычислительная сложность.

Целью работы является разработка метода пространственно-временной хаотической параметризации движения на основе клеточных автоматов для построения модели мобильности локальной сети с хаотическим движением узлов.

Модели мобильности с независимым движением узлов

Для описания независимого движения узлов используются следующие модели.

Модель мобильности со случайным (броуновским) движением узлов [1]. Это одна из первых моделей мобильности, основанная на непредсказуемом характере движения узлов. В данной модели скорость и направление перемещения выбираются случайным образом. Изменение скорости и направления движения происходит через равные промежутки времени или через заданное постоянное пройденное расстояние. Случайное изменение параметров движения позволяет снизить вычислительную сложность построения модели. Однако в результате может моделироваться нереалистичное движение, например с внезапными остановками и резкими поворотами.

Модель мобильности со случайными точками маршрута [5]. Эта модель учитывает паузы между изменениями направления и/или скорости движения. Сначала узел находится в состоянии покоя определенное время (время покоя), затем выбирает случайным образом точку в области моделирования и скорость и движется к данной точке. При достижении заданной точки узел опять находится в состоянии покоя перед началом нового цикла движения. Если время покоя равно нулю, то данная модель сводится к предыдущей модели. Недостатком данной модели является сложность выбора значений времени покоя и скорости.

Модель мобильности со случайным направлением движения [6]. Недостатками предыдущих моделей является группирование узлов в определенной области моделирования и прохождение через центр траекторий движения. Данные недостатки устраняет модель со случайным направлением движения. В ней узел выбирает случайное направление и движется до границы области моделирования, где он останавливается на некоторое время и затем выбирает новое направление, после чего процесс повторяется.

Модель мобильности Гаусса-Маркова [7]. Данная модель позволяет избежать резких изменений траектории движения за счет учета текущих параметров движения (скорости и направления) при вычислении параметров движения в следующий момент времени. Первоначально каждому узлу назначаются текущая скорость и направление. Их изменение происходит в фиксированные моменты времени.

Общим недостатком рассмотренных моделей является независимость параметров движения любого узла от параметров движения соседних узлов. В реальных условиях проявляется пространственно-временная хаотическая динамика параметров движения узлов.

Модели мобильности с групповым движением узлов

В некоторых условиях мобильные узлы движутся в группе. Для моделирования такого движения узлов используются групповые модели мобильности.

Модель мобильности при движении в колонне [7]. В такой модели задается опорная линия с соответствующими каждому узлу опорными точками, в результате чего формируется колонна узлов. Узлы могут двигаться случайным образом вокруг опорных точек. При перемещении опорной линии узлы следуют за своими опорными точками. Примером такого движения является перемещение колонны транспортных средств.

Кочевая модель мобильности [8]. В кочевой модели мобильности узлы движутся по индивидуальному случайному пути от одной опорной точки к другой. При достижении опорной точки узлы движутся возле нее некоторое время. Примером такой модели может быть группа экскурсантов в музее, которая движется от одного экспоната к другому и задерживается возле каждого экспоната на некоторое время.

Модель мобильности с преследованием [6]. Такая модель может использоваться для моделирования движения узлов, которые преследуют некоторую цель. В отличие от предыдущей модели узлам не ставится задача выйти точно к преследуемому узлу, а допускается отклонение, задаваемое случайным вектором.

Модель мобильности с групповой опорной точкой [9]. Данная модель описывает случайное движение группы узлов и каждого отдельного узла в пределах группы. Групповое движение

базируется на пути, пройденном условным центром группы (групповой опорной точки), а индивидуальное движение базируется на перемещении индивидуальных опорных точек, которые перемещаются вместе с логическим центром. Примером такого движения может служить стая птиц в небе.

Основным недостатком данных моделей является использование только одной группы. При одновременном использовании нескольких таких моделей для описания движения соответствующего числа групп узлов в общем пространстве их параметры движения оказываются некоррелированными.

Пространственно-временная хаотическая параметризация движения на основе клеточных автоматов

Для построения модели мобильности локальной сети с хаотическим движением узлов предлагается метод пространственно-временной хаотической параметризации движения точек в двухмерном пространстве размером $Y \times X$ на основе клеточных автоматов. Сущность метода состоит в использовании двух многослойных клеточных автоматов $C_Y(t) = \left\| c_Y(d,y,x,t) \right\|_{\left(d=\overline{1,D}, y=\overline{0,Y_C-1}, x=\overline{0,X_C-1}\right)}$ и $C_X(t) = \left\| c_X(d,y,x,t) \right\|_{\left(d=\overline{1,D}, y=\overline{0,Y_C-1}, x=\overline{0,X_C-1}\right)}$ для определения вектора $A(y,x,t) = \left(a_Y(y,x,t), a_X(y,x,t)\right)$ ускорения для каждой точки (y,x) двухмерного хаотического пространства. Число *D* слоев многослойных клеточных автоматов определяет точность представления компонент $\left(a_Y(y,x,t), a_X(y,x,t)\right)$ вектора ускорения. Метод обеспечивает хаотическое изменение параметров движения для произвольного числа узлов локальной мобильной сети за счет определения пространственно-временной хаотической динамики во всех точках пространства.

Алгоритм, реализующий предлагаемый метод пространственно-временной хаотической параметризации движения точек, состоит из следующих шагов.

1. Инициализация многослойных клеточных автоматов. С использованием генератора случайных чисел задаются начальные состояния $(t=0)$ клеточных автоматов $C_Y(t)$ и $C_X(t)$, где $t = \overline{0,T-1}$ – счетчик циклов моделирования; T – число циклов моделирования.

2. Инициализация мобильных узлов в хаотическом пространстве. С помощью генератора случайных чисел для каждого *n*-го узла (где $n = \overline{0,N-1}$; N – число узлов) при $t=0$ задается набор $M(n,t) = \left(y(n,t), x(n,t), v_Y(n,t), v_X(n,t)\right)$ параметров движения, где $\left(y(n,t), x(n,t)\right)$ – текущие координаты *n*-го узла; $\left(v_Y(n,t), v_X(n,t)\right)$ – компоненты вектора скорости $V(n,t)$.

3. Начало цикла моделирования хаотического движения. Приращение значения счетчика циклов моделирования: $t = t+1$.

4. Вычисление текущих состояний клеточных автоматов $C_Y(t)$ и $C_X(t)$.

5. Переопределение компонент вектора скорости $V(n,t)$ *n*-го узла для $n = \overline{0,N-1}$ с помощью выражения

$$\begin{cases} v_Y(n,t) = f\left(v_Y(n,t-1), c_Y\left(d, y(n,t), x(n,t), t\right)\right), \\ v_X(n,t) = f\left(v_X(n,t-1), c_X\left(d, y(n,t), x(n,t), t\right)\right). \end{cases} \quad (1)$$

6. Переопределение текущих координат $\left(y(n,t),\ x(n,t)\right)$ *n*-го узла для $n = \overline{0,N-1}$ с помощью выражения

$$\begin{cases} y(n,t) = y(n,t-1) + v_Y(n,t), \\ x(n,t) = x(n,t-1) + v_X(n,t). \end{cases} \quad (2)$$

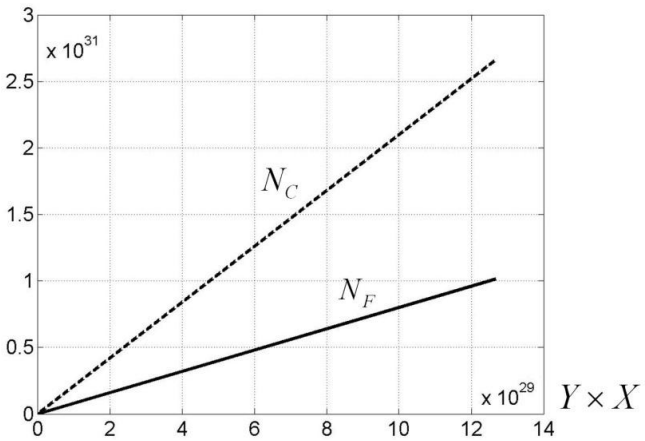
7. Конец цикла. Проверка условия $t < T$. Если условие выполняется, то осуществляется переход на шаг 3. Иначе – выход из цикла.

В результате выполнения данного алгоритма реализуется модель мобильности с хаотическим движением точек.

Основным недостатком клеточного автомата, в том числе многослойного, является высокая вероятность вырождения хаотической динамики. Однако, как показано в [10], хаотическая динамика может быть стабилизирована в многослойном клеточном автомате с дополнительными связями между слоями.

Одной из основных проблем моделирования хаотического движения узлов на основе клеточного автомата и других известных генераторов хаоса является рост вычислительной сложности с увеличением размера хаотического пространства, что связано с формированием пространственной хаотической динамики для всех точек пространства и приводит к увеличению объема оперативной памяти для хранения состояний генератора хаоса. Для снижения вычислительной сложности пространственно-временной хаотической параметризации движения точек предлагается использовать фрактальное расширение хаотического пространства с помощью рекурсивных перестановок. Сущность данного подхода состоит в использовании хаотического пространства небольшого размера для формирования хаотического пространства произвольного размера в результате фрактального расширения и рекурсивной перестановки элементов исходного хаотического пространства. Это позволяет сократить вычислительную сложность формирования хаотического пространства требуемого размера за счет уменьшения числа операций при фрактальном расширении исходного хаотического пространства и сохранить характер пространственно-временной хаотической динамики за счет рекурсивных перестановок, поддерживающих локальную связь точек хаотического пространства после перестановки.

Проведен анализ зависимостей числа операций, необходимых для формирования хаотического пространства, от размера $Y \times X$ хаотического пространства (см. рисунок) при использовании обычного клеточного автомата (кривая N_C) и фрактального расширения исходного хаотического пространства небольшого размера с помощью рекурсивных перестановок (кривая N_F).



Зависимости числа операций от размера формируемого хаотического пространства

Из рисунка следует, что фрактальное расширение хаотического пространства клеточного автомата позволяет в 2,5 раза уменьшить вычислительную сложность формирования пространственно-временной хаотической динамики в пространстве заданного размера по сравнению с базовым подходом, использующим для формирования хаотического пространства обычный клеточный автомат.

Заключение

Предложен метод пространственно-временной хаотической параметризации движения точек в двухмерном пространстве на основе клеточных автоматов для построения модели мобильности локальной сети с хаотическим движением узлов. Сущность метода состоит в использовании двух многослойных клеточных автоматов для определения вектора ускорения для каждой точки двухмерного хаотического пространства. Число слоев многослойных клеточных автоматов определяет точность представления компонент вектора ускорения. Метод обеспечивает хаотическое изменение параметров движения для произвольного числа узлов локальной мобильной сети за счет определения пространственно-временной хаотической динамики во всех точках

пространства. Для снижения вычислительной сложности пространственно-временной хаотической параметризации движения точек предложено использовать фрактальное расширение хаотического пространства с помощью рекурсивных перестановок. Показано, что это позволяет в 2,5 раза сократить вычислительную сложность формирования хаотического пространства требуемого размера за счет уменьшения числа операций при фрактальном расширении исходного хаотического пространства и сохранить характер пространственно-временной хаотической динамики за счет рекурсивных перестановок, поддерживающих локальную связь точек хаотического пространства после перестановки.

MOTION SIMULATION OF NODES IN LOCAL MOBILE NETWORK BASED ON DYNAMIC CHAOS

A.A. PODLUTSKI, V.Yu. TSVIATKOU, K.T.H. AL-SHAMERY

Abstract

A method of space-time chaotic parameterization of the points in a two dimensional space on the basis of cellular automata to model a wireless LAN with the random movement of nodes is proposed. The method provides a chaotic change in the parameters of motion for an arbitrary number of hosts in the local mobile network by identifying spatiotemporal chaotic dynamics for all points in space. It is shown that in order to reduce the computational complexity of the spatial-temporal chaotic motion parameterization can be used fractal expansion of chaotic space by using recursive permutations.

Литература

1. *Camp T., Boleng J., Davies V.* // Wireless Communications and Mobile Computing. 2002. Vol. 2. P. 483-502.
2. *Ahmad A.* // International Journal on Computer Science and Engineering. 2009. Vol. 2 (1). P. 46-50.
3. *Toosizadeh S.* // International Conference on Computer and Software Modeling. IPCSIT Press, Singapore. 2011. Vol. 14. P. 43-47.
4. *Silva C.P.* // Proc. of IEEE Aerospace Conference. 2000. P. 279-299.
5. *Jonson D., Maltz D.* // Mobile Computing, 1996. P. 153-181.
6. *Royer E., Melliar-Smith PM, Moser L.* // In Proceedings of the IEEE International Conference on Communications (ICC). 2001.
7. *Liang B, Haas Z.* // In Proceedings of the Joint Conference of the IEEE Computer and Communications Societies (INFOCOM). 1999.
8. *Karp B.* // In Proceedings of the ACM International Workshop on Modeling and Simulation of Wireless and Mobile Systems (MSWiM). 1999.
9. *Борискевич А.А.* // Доклады бел. гос. университета информатики и радиоэлектроники. 2006. №6 (12). С. 30-39.

УДК 621.391

ФОРМИРОВАНИЕ ТРЕХМЕРНОГО ФРАКТАЛЬНОГО ХАОСА НА ОСНОВЕ КЛЕТОЧНОГО АВТОМАТА

А.А. ЮРЕВИЧ, А.Д. КИМ

Белорусский государственный университет информатики и радиоэлектроники
П. Бровки, 6, Минск, 220013, Беларусь

Поступила в редакцию 24 апреля 2012

Предложен метод формирования трехмерных фрактальных хаотических образов на основе клеточного автомата и рекурсивных перестановок. Сущность метода состоит в использовании клеточного автомата небольшого размера для формирования трехмерных хаотических образов произвольного размера в результате фрактального расширения и рекурсивной перестановки элементов матрицы состояний клеточного автомата на каждом такте его работы. Показано, что метод обеспечивает уменьшение вычислительной сложности формирования хаотических образов.

Ключевые слова: фрактальный хаос, клеточный автомат, рекурсивные перестановки.

Введение

Трехмерные хаотические образы применяются в задачах шифрования изображений [1], моделирования физических процессов [2], обработки сигналов [3]. Их недостатком является высокая вычислительная сложность. Снижение вычислительной сложности формирования хаотических образов возможно за счет фрактального расширения исходного хаотического пространства малой размерности. Для его построения использован простейший алгоритм на основе модели клеточного автомата. Для уменьшения блочного эффекта от фрактального расширения матрицы, предлагается использовать рекурсивные перестановки элементов матрицы.

Целью работы является разработка вычислительно простого метода формирования трехмерного фрактального хаоса на основе клеточного автомата и рекурсивных перестановок.

Клеточные автоматы

Клеточный автомат [4] представляет собой итеративную модель неструктурированного динамического хаоса, которая рассматривается в трехмерном бинарном пространстве размером $Z_C \times Y_C \times X_C$. Состояния элементов пространства на итерации t описываются хаотической матрицей $C(t) = \left\| c(z,y,x,t) \right\|_{\left(z=\overline{0,Z_C-1},\, y=\overline{0,Y_C-1},\, x=\overline{0,X_C-1}\right)}$, значения элементов которой рассчитываются по выражению

$$c(y,x,t) = \begin{cases} 1, \text{ при } \Big(\big(c(z,y,x,t-1)=0\big) \wedge \big(\mathrm{sum}(z,y,x,t)=\theta_B\big)\Big) \vee \\ \qquad \vee \Big(\big(c(z,y,x,t-1)=1\big) \wedge \big(\theta_L \le \mathrm{sum}(z,y,x,t) \le \theta_H\big)\Big), \\ 0, \text{ при } \Big(\big(c(z,y,x,t-1)=0\big) \wedge \big(\mathrm{sum}(z,y,x,t) \ne \theta_B\big)\Big) \vee \\ \qquad \vee \Big(\big(c(z,y,x,t-1)=1\big) \wedge \neg\big(\theta_L \le \mathrm{sum}(z,y,x,t) \le \theta_H\big)\Big) \end{cases} \quad (1)$$

при $z=\overline{0,Z_C-1}$, $y=\overline{0,Y_C-1}$, $x=\overline{0,X_C-1}$, $t=\overline{1,T}$, где T – число формируемых хаотических образов (число итераций); θ_B – порог рождения; θ_L, θ_H – пороговые значения жизни; $\mathrm{sum}(z,y,x,t)=\sum_{k=\mathrm{mod}_{Z_C(z-1)}}^{\mathrm{mod}_{Z_C(z+1)}}\sum_{j=\mathrm{mod}_{Y_C(y-1)}}^{\mathrm{mod}_{Y_C(y+1)}}\sum_{i=\mathrm{mod}_{X_C(x-1)}}^{\mathrm{mod}_{X_C(x+1)}}c(k,j,i,t-1)-c(z,y,x,t-1)$ – сумма элементов хаотической матрицы в окрестности элемента относительно $c(z,y,x,t-1)$; $C(0)$ – хаотическая матрица на итерации 0.

Для формируемой клеточным автоматом последовательности хаотических образов высока вероятность вырождения хаотической динамики. Хаотическая динамика стабилизи-руется [5] в многослойном клеточном автомате с дополнительными связями между слоями.

Рекурсивные перестановки

Рекурсивные перестановки задают фрактальный порядок выборки элементов матрицы, который описывает развертку *N*-мерного пространства в одномерное. Фрактальность развертки обеспечивает корреляцию между элементами исходного пространства в одномерном представлении после преобразования. Примером рекурсивной развертки с непрерывной траекторией (заполняющей пространство кривой) является развертка Гильберта (рис. 1) [6].

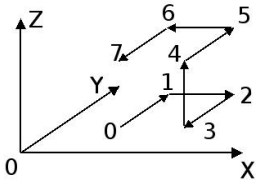


Рис. 1. Примитив рекурсивной развертки Гильберта

Матрица рекурсивной перестановки формируется вычислительно простым способом с помощью рекуррентного преобразования из матрицы примитива и множества матриц его ориентации. Примитив задает тип, исходную точку и траекторию рекурсивной развертки. Рекуррентное преобразование задает закон фрактального расширения матрицы примитива.

Метод формирования фрактальных хаотических образов

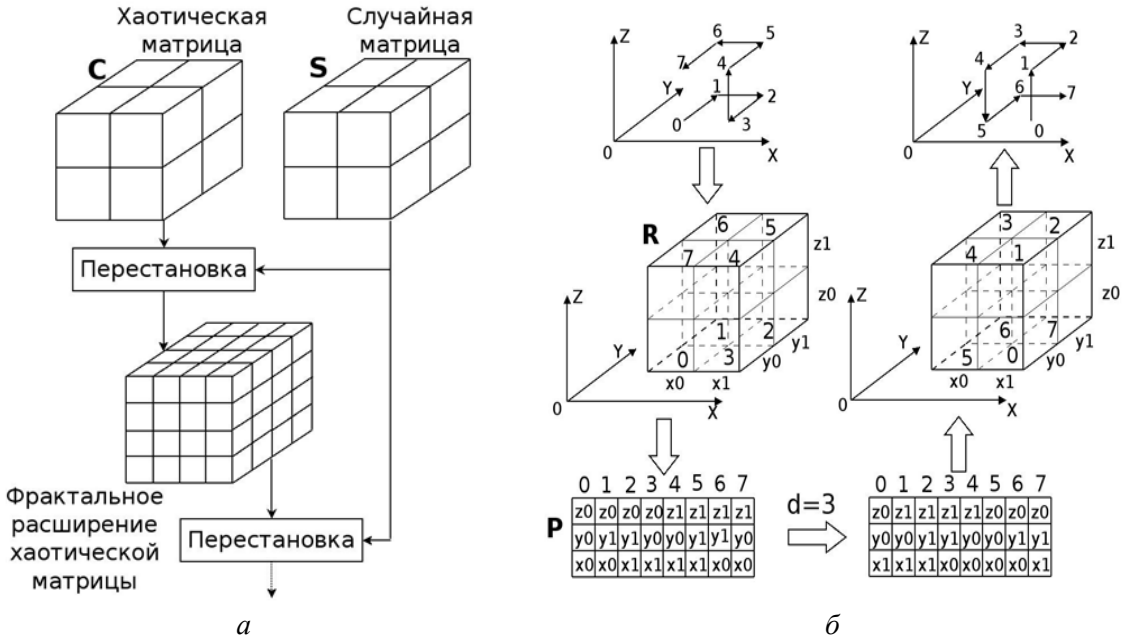
Предлагается метод формирования фрактальных хаотических образов на основе клеточного автомата и рекурсивных перестановок. Суть метода состоит в использовании модели клеточного автомата небольшого размера для формирования хаотических образов произвольного размера за счет фрактального расширения и рекурсивной перестановки элементов матрицы его состояний на каждой итерации. Метод сокращает вычислительную сложность формирования образов за счет уменьшения числа операций.

Алгоритм реализации предлагаемого метода состоит из следующих шагов.

1. Формирование и инициализация значений бинарной хаотической матрицы $C(t)=\left\|c(z,y,x,t)\right\|_{\left(z=\overline{0,Z-1},y=\overline{0,Y-1},x=\overline{0,X-1}\right)}$ на итерации $t=0$, где Z, Y, X – размеры хаотической матрицы в трехмерном пространстве; $t=\overline{0,T}$; T – число итераций. Матрица $C(t)$ является ядром фрактального расширения на каждой итерации (рис. 2,*а*).

2. Формирование и инициализация значений случайной матрицы $S(t)=\left\|s(z,y,x,t)\right\|_{\left(z=\overline{0,Z-1},y=\overline{0,Y-1},x=\overline{0,X-1}\right)}$ на итерации $t=0$ для определения величины циклического сдвига элементов хаотической матрицы $C(t)$.

3. Формирование и инициализация значений рекурсивной матрицы $R=\left\|r(z,y,x)\right\|_{\left(z=\overline{0,Z-1},y=\overline{0,Y-1},x=\overline{0,X-1}\right)}$, содержащей целые числа в интервале $[0,Z\times Y\times X-1]$. Расположение чисел определяет порядок выборки элементов матрицы R (рис. 2,*б*). Матрица R необходима для задания правила циклического сдвига элементов хаотической матрицы $C(t)$. Основное ограничение для правил циклического сдвига – сохранение окрестности. Ограничению удовлетворяют рекурсивные перестановки на основе разверток Гильберта.



а *б*

Рис. 2. Формирование фрактального хаоса: фрактальное расширение хаотической матрицы (*а*); рекурсивный циклический сдвиг элементов хаотической матрицы (*б*)

4. Формирование и инициализация координатного вектора $P = \left\| \left(p_Z(i), p_Y(i), p_X(i) \right) \right\|_{\left(i=\overline{0, Z \times Y \times X - 1}\right)}$, значения элементов которого связаны со значениями элементов рекурсивной матрицы R в соответствии с соотношением

$$\forall z \forall y \forall x \forall i \left(r(z,y,x) = i \right) \leftrightarrow \left(\left(p_Z(i) = z \right) \wedge \left(p_Y(i) = y \right) \wedge \left(p_X(i) = x \right) \right). \quad (2)$$

Координатный вектор P необходим для реализации рекурсивного циклического сдвига элементов хаотической матрицы $C(t)$ по правилу, заданному в рекурсивной матрице R.

5. Инициализация счетчика итераций $t = 1$.

6. Начало цикла формирования фрактальных хаотических образов. Пересчет значений хаотической матрицы $C(t)$ на основе модели клеточного автомата по выражению (1).

7. Пересчет значений случайной матрицы $S(t)$ с помощью выражения

$$s(z,y,x,t) = \mathrm{mod}_{ZYX} \left(c(z,y,x,t) + s(z,y,x,t-1) \right) \quad (3)$$

при $z = \overline{0, Z-1}$, $y = \overline{0, Y-1}$, $x = \overline{0, X-1}$.

8. Формирование и инициализация значений фрактальной хаотической матрицы $F(l,t) = \left\| f(z,y,x,l,t) \right\|_{\left(z=\overline{0, Z^{l+1}-1}, y=\overline{0, Y^{l+1}-1}, x=\overline{0, X^{l+1}-1}\right)}$ на уровне $l = 0$, где $l = \overline{0, L-1}$; L – число уровней фрактального расширения. Значениям фрактальной хаотической матрицы $F(0,t)$ присваиваются значения исходной хаотической матрицы $C(t)$: $f(z,y,x,0,t) = c(z,y,x,t)$ при $z = \overline{0, Z-1}$, $y = \overline{0, Y-1}$, $x = \overline{0, X-1}$. Число L уровней фрактального расширения определяется исходя из размеров $Z \times Y \times X$ исходной хаотической матрицы $C(t)$ и размеров $Z_C \times Y_C \times X_C$ результирующей фрактальной хаотической матрицы $F(L,t)$ с помощью выражения

$$L = \max \left(\lceil \log_Z Z_C \rceil, \lceil \log_Y Y_C \rceil, \lceil \log_X X_C \rceil \right), \quad (4)$$

где $\lceil \ \rceil$ – операция округления до ближайшего целого числа с избытком.

9. Инициализация счетчика уровней фрактального расширения $l = 1$.

10. Начало цикла фрактального расширения хаотической матрицы. Формирование фрактальной хаотической матрицы $F(l,t)$ на уровне l и вычисление ее значений по выражению

$$f(z,y,x,l,t)=c\left(p_Z\left(\mathrm{mod}_Z(d+z)\right),p_Y\left(\mathrm{mod}_Y(d+y)\right),p_X\left(\mathrm{mod}_X(d+x)\right)\right), \quad (5)$$

где $d=s\left(\lfloor z/Z\rfloor,\lfloor y/Y\rfloor,\lfloor x/X\rfloor\right)+f\left(\lfloor z/Z^l\rfloor,\lfloor y/Y^l\rfloor,\lfloor x/X^l\rfloor,l-1\right)$ – величина циклического сдвига элементов хаотической матрицы $C(t)$ по правилу рекурсивной перестановки (при $z=\overline{0,Z^{l+1}-1}$, $y=\overline{0,Y^{l+1}-1}$, $x=\overline{0,X^{l+1}-1}$), заданному рекурсивной матрицей R и координатным вектором P; $\lfloor\ \rfloor$ – операция округления до ближайшего целого с недостатком. За счет фрактального расширения ZYX элементам матрицы $F(l,t)$ соответствуют одни и те же значения $s\left(\lfloor z/Z\rfloor,\lfloor y/Y\rfloor,\lfloor x/X\rfloor\right)$ и $f\left(\lfloor z/Z^l\rfloor,\lfloor y/Y^l\rfloor,\lfloor x/X^l\rfloor,l-1\right)$, т.е. на l-м уровне фрактального расширения для $Z^{l+1}Y^{l+1}X^{l+1}$ элементов матрицы $F(l,t)$ рассчитываются только $Z^lY^lX^l$ значений циклического сдвига d.

11. Приращение значения счетчика уровней фрактального расширения $l=l+1$.

12. Проверка условия $l<L$. Если условие выполняется, то осуществляется переход на шаг 10, а иначе – окончание цикла фрактального расширения хаотической матрицы.

13. Приращение значения счетчика итераций $t=t+1$.

14. Проверка условия $t\le T$. Если условие выполняется, то осуществляется переход на шаг 6, а иначе – окончание цикла формирования образов и алгоритма.

В результате формируется множество фрактальных хаотических матриц $F(L,t)$ при $t=\overline{0,T}$ размером $Z_C\times Y_C\times X_C=Z^{L+1}\times Y^{L+1}\times X^{L+1}$, состоящих из $Z^L\times Y^L\times X^L$ преобразованных исходных хаотических матриц $C(t)$, элементы которых циклически сдвинуты по правилу рекурсивной перестановки, обеспечивающей сохранение локальной корреляции элементов исходной хаотической матрицы.

Оценка эффективности метода формирования фрактального хаоса

Для оценки эффективности предложенного метода формирования фрактальных хаотических образов на основе клеточного автомата и рекурсивных перестановок произведено его сравнение с базовым методом формирования неструктурированных хаотических образов на основе клеточного автомата. В качестве сопоставляемого параметра использована вычислительная сложность формирования результирующей хаотической матрицы.

Из выражения (1) следует, что для вычисления значения одного элемента хаотической матрицы базовым методом на основе клеточного автомата необходимо 57 операций. Для формирования хаотического образа размером $Z_CY_CX_C$ требуется число N_C операций, определяемое с помощью выражения

$$N_C=57Z_CY_CX_C. \quad (6)$$

Число N_F операций для формирования фрактального хаотического образа на основе клеточного автомата и рекурсивных перестановок определяется с помощью выражения

$$N_F=\sum_{i=6}^{9}N_S(i)+\sum_{l=1}^{L-1}\sum_{i=10}^{12}N_S(i,l)=64ZYX-3+4L+15\sum_{l=1}^{L-1}Z^lY^lX^l+11\sum_{l=1}^{L-1}Z^{l+1}Y^{l+1}X^{l+1}, \quad (7)$$

где $N_S(i)$, $N_S(i,l)$ – число операций на шаге i алгоритма образов (см. таблицу). Значения $N_S(i)$ и $N_S(i,l)$ учитывают операции извлечения из памяти O_{MR}, сложения O_A, сравнения O_C, по модулю O_M, записи в память O_{MS}, деления O_D, округления до ближайшего целого O_R.

Число операций в алгоритме формирования фрактальных хаотических образов

Шаги алгоритма, i	Выражения для определения числа $N_S(i)$ или $N_S(i,l)$ операций	Схема вычисления (индекс перед обозначением операции указывает на количество операций)
6	$N_S(6) = 57ZYX$	$(27O_{MR} + 26O_A + 3O_C + 1O_{MS})ZYX$
7	$N_S(7) = 5ZYX$	$(2O_{MR} + 1O_A + 1O_M + 1O_{MS})ZYX$
8	$N_S(8) = 2ZYX$	$(1O_{MR} + 1O_{MS})ZYX$
9	$N_S(9) = 1$	$1O_{MS}$
10	$N_S(10,l) = 15Z^lY^lX^l + 11Z^{l+1}Y^{l+1}X^{l+1}$	$(6O_D + 6O_R + 2O_{MR} + 1O_A)Z^lY^lX^l +$ $+(3O_M + 3O_A + 4O_{MR} + O_{MS})Z^{l+1}Y^{l+1}X^{l+1}$
11	$N_S(11,l) = 3$	$1O_{MR} + 1O_A + 1O_{MS}$
12	$N_S(12,l) = 1$	$1O_C$

На рис. 3 представлены зависимости числа операций N_F (сплошной линией) и N_C (прерывистой линией) от размера $Z_C \times Y_C \times X_C$ формируемой хаотической матрицы при фиксированном размере ядра фрактального расширения. Предложенный метод формирования образов на основе клеточного автомата и рекурсивных перестановок уменьшает вычислительную сложность до 5 раз по сравнению с базовым методом на основе клеточного автомата.

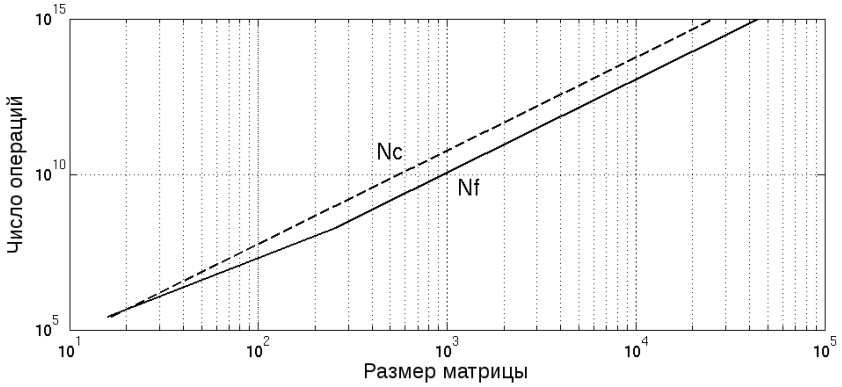


Рис. 3. Зависимость числа операций от размера формируемой хаотической матрицы

Заключение

Предложен метод формирования фрактальных хаотических образов на основе клеточного автомата и рекурсивных перестановок. Сущность метода состоит в использовании клеточного автомата небольшого размера для формирования хаотических образов произвольного размера в результате фрактального расширения и рекурсивной перестановки элементов матрицы состояний клеточного автомата на каждом такте его работы. Установлено, что метод обеспечивает уменьшение вычислительной сложности формирования хаотических образов до 5 раз по сравнению с методом на основе модели клеточного автомата.

GENERATION OF THREE-DIMENSIONAL FRACTAL CHAOS BASED ON CELLULAR AUTOMATON

A.A. YUREVICH, A.D. KIM

Abstract

A generator of three-dimensional chaos is proposed in this paper. The generator is based on fractal widening of the small kernel matrix and cellular automaton. The alignment effect is minimized by cyclic shifting of the state matrix elements. An estimation of the computational complexity of the generator is presented. It is shown that this generator compared to the three-dimensional chaos generator based on cellular automaton provides a reduction in the computational complexity.

Литература

1. *Ahmad A.A.* // International Journal on Computer Science and Engineering. 2009. Vol. 2 (1). P. 46-50.
2. *Toosizadeh S.* // International Conference on Computer and Software Modeling. 2011. Vol. 14. P. 43-47.
3. *Silva C.P.* // Proc. of IEEE Aerospace Conference. 2000. P. 279-299.
4. *Тоффоли Т.* Машины клеточных автоматов. М., 1991.
5. *Борискевич А.А., Горнович И.Л., Цветков В.Ю.* // Докл. БГУИР. 2006. №6. С. 30-39.
6. *Bader M.* // Springer-Verlag New York Inc. 2012. P. 18-27.

УДК 621.391.14

ПРИМЕНЕНИЕ НОРМ СИНДРОМОВ ДЛЯ ИДЕНТИФИКАЦИИ КРАТНОСТИ ОШИБОК ПРИ КОРРЕКЦИИ СТИРАНИЙ БЧХ-КОДАМИ

Н.А. САЛАС, В.К. КОНОПЕЛЬКО, А.И. КОРОЛЕВ

Белорусский государственный университет информатики и радиоэлектроники
П. Бровки, 6, Минск, 220013, Беларусь

Поступила в редакцию 12 марта 2012

Рассматривается коррекция многократных стираний на основе идентификации кратности несогласованных стертых символов норменным методом в двух каналах (прямом и инверсном) декодирования. Показано, что использование норм синдромов для идентификации кратности несогласованных стираний БЧХ-кодами позволяет эффективно и быстро определить их кратность при кратности стираний $t_c \le 5$. Установлено, что предложенный способ декодирования позволяет уменьшить более чем в 3 раза сложность декодирования по сравнению с известным методом коррекции стираний, основанным на решении систем уравнений в полях Галуа.

Ключевые слова: ошибки, согласованные стирания, несогласованные стирания, идентификация, декодер, синдром, норма синдромов.

Введение

В настоящее время одним из способов избежать так называемую «проблему селектора», возникающую при увеличении кратности исправляемых ошибок в телекоммуникационных системах является использование понятия «стирания». Под стиранием понимаются искаженные символы, местоположение которых известно при декодировании, но неизвестно их истинное значение. Известно, что для исправления стираний требуется вдвое меньшая избыточность, чем при исправлении ошибок той же кратности [1]. Однако реализация устройств коррекции стираний сопряжена с высокими вычислительными затратами из-за необходимости перебора значений символов в разрядах стираний для нахождения синдрома S=0 [2].

В данной статье предлагается способ исправления многократных стираний как ошибок на основе анализа синдромов ошибок, использование контроля четности и норм синдромов для идентификации кратности ошибок в двух каналах декодирования (прямом и инверсном). Это позволяет уменьшить аппаратурную сложность декодирования.

Коррекция стираний как ошибок

Существует несколько простых методов коррекции стираний с использованием линейных кодов. Сущность данных методов состоит, как правило, в переборе всех возможных сочетаний стертых символов с последовательным вычислением синдрома до тех пор, пока синдром не будет равен нулю. Очевидно, что этот процесс требует больших временных затрат [2]. В [3] предложено решение по исправлению стираний, заключающееся в вычислении вектора согласования путем решения соответствующих уравнений, что позволяет увеличить быстродействие. Однако реализация устройства декодирования требует больших аппаратурных затрат. Вместе с тем, использование понятий согласованных и несогласованных стираний при коррекции многократных стираний, позволяет за счет инверсии переводит в согласованные стирания в несогласованные и наоборот. Благодаря этому появляется возможность выбирать для коррек-

ции слова, в которых имеется меньшее количество несогласованных стираний (ошибок), и корректировать их известными методами.

Необходимым условием такой идентификации многократных несогласованных стираний служат коды, словами которых являются как прямые, так и инверсные слова, например, транспарантные коды Хэмминга [1]. Нетрудно проверить, что БЧХ-код, задаваемый проверочной матрицей $H = \left[\alpha^z, \alpha^{3z}\right]^T$, где первая подматрица задает код Хэмминга, а вторая подматрица – код Хэмминга с переставленными позициями, является транспарантным, поскольку среди кодовых слов данного БХЧ-кода имеется слово, состоящее из единичных символов $A_1 = (1,1,....,1)$.

Коррекция стираний с идентификацией кратности ошибок в прямом и инверсном словах

Сложность реализации декодирующего устройства можно уменьшить, применив при его построении два регистра для хранения и одновременной обработки прямого и инверсного кодовых слов, содержащих стирания (см. рис. 1).

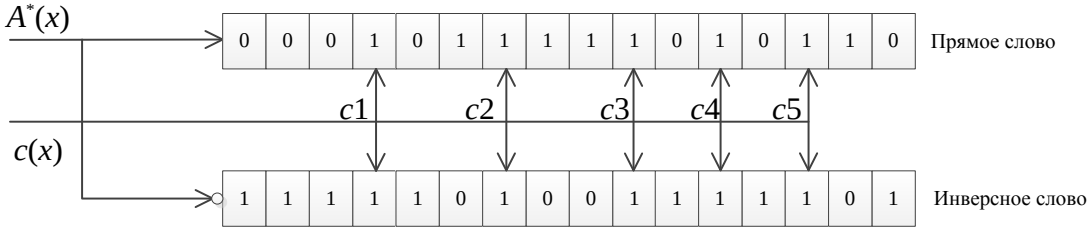


Рис. 1. Значения символов в стертых позициях прямого и инверсного слов

Из рис. 1 следует, что на стертых позициях прямого и инверсного слов содержатся одни и те же значения. Это позволяет выбирать для дальнейшей обработки слово с меньшим количеством произошедших ошибок (несогласованных стираний) и, соответственно, анализировать меньшее количество синдромов в селекторе декодера. Очевидно, что для осуществления этого решения необходимо использовать идентификацию кратности ошибок в прямом и инверсном словах. В качестве идентификационных параметров можно использовать синдромы и их нормы, а также разряд контроля четности в прямом и инверсном кодовых словах. Рассмотрим подробнее возможность использования этих идентификаторов для однозначного определения кратности несогласованных стираний при $t_c \le 5$.

Для коррекции стираний кратности t_c=5 необходимо использовать код с d=6, т.е. БЧХ-код с d=5, дополненный контролем четности:

$$H = \left[\begin{array}{ccc|c} & H_{\text{БЧХ}} & & \begin{matrix}1\\1\\1\end{matrix} \\ \hline 1 & 1 & 1 & 1 \end{array}\right]$$

Идентификационные признаки для стираний кратности t_c=5 приведены в табл. 1, где $t_и$ – количество несогласованных стираний (ошибок) в прямом и инверсном регистрах, S_1^1, S_1^2 – синдромы прямого и инверсного слов, $S_ч^1$, $S_ч^2$ – контроль на четность прямого и инверсного слов.

Таблица 1. **Идентификационные признаки стираний кратности t_c=5**

№	Число несогласованных стираний $t_и$ в		S_1^1	$S_ч^1$	S_1^2	$S_ч^2$	Корректируемое слово
	прямом слове	инверсном слове					
1	5	0	1	1	0	0	инверсное слово
2	4	1	1	0	1	1	-
3	3	2	1	1	1	0	-
4	2	3	1	0	1	1	-
5	1	4	1	1	1	0	-
6	0	5	0	0	1	1	прямое слово

Из табл. 1 видно, что для стираний кратности $t_и$=(4, 1) и $t_и$=(2, 3) идентификационные признаки одинаковы и равны (1 0 1 1), что не позволяет однозначно определить вид произошедших ошибок. Аналогично происходит для стираний $t_и$=(3, 2) и $t_и$=(1, 4). Отсюда следует, что для идентификации ошибок кратности t_c=5 требуется введение дополнительных отличительных признаков. Таким признаком может быть норма синдрома N.

Для БЧХ-кода с минимальным кодовым расстоянием d=5, задаваемого проверочной матрицей $H=\left[\alpha^z,\alpha^{3z}\right]^T$ и синдромом $S=\left[\alpha^i,\alpha^j\right]^T$, норма синдрома равна $N=\left(j-3i\right)\bmod n$, где n – длина кода [1, 4, 5]. Для одиночных ошибок норма не зависит от местоположения ошибок и всегда равна нулю $\left(N=0\right)$, для двухкратных ошибок – значения нормы не равны нулю и различны. Для трехкратных ошибок синдром $S_3\neq 0$, а также некоторые нормы не вычисляются, т.к. $S_1=0$. Таким образом, введя нормы синдромов в качестве признака кратности ошибок, получим приведенные в табл. 2 идентификационные признаки, где N^1, N^2 – норма синдромов прямого и инверсного слов.

Таблица 2. **Идентификационные признаки стираний кратности t_c=5 с нормами синдромов N**

№	Число несогласованных стираний $t_и$ в		S_1^1	$S_ч^1$	S_1^2	$S_ч^2$	N^1	N^2	Корректируемое слово
	прямом слове	инверсном слове							
1	t_c=5	t_c=0	1	1	0	0	≠0	-	инверсное слово
2	t_c=4	t_c=1	1	0	1	1	≠0	0	инверсное слово
3	t_c=3	t_c=2	1	1	1	0	≠0	≠0	инверсное слово
4	t_c=2	t_c=3	1	0	1	1	≠0	≠0	прямое слово
5	t_c=1	t_c=4	1	1	1	0	0	≠0	прямое слово
6	t_c=0	t_c=5	0	0	1	1	-	≠0	прямое слово

Анализ данных табл. 2 показывает, что по вычисленным синдромам и их нормам можно однозначно идентифицировать количество ошибок в прямом и инверсном регистрах на основании нижеследующего правила и правильно выбрать нужное слово для декодирования.

Декодирование осуществляется по информации в инверсном регистре, в следующих случаях:

1. если $\left(S_1^1,S_ч^1\right)=(1,1)$, $\left(S_1^2,S_ч^2\right)=(0,0)$;

2. при $\left(S_1^1,S_ч^1\right)=(1,0)$, $\left(S_1^2,S_ч^2\right)=(1,1)$, $N^2=0$;

3. если $\left(S_1^1,S_ч^1\right)=(1,1)$, $\left(S_1^2,S_ч^2\right)=(1,0)$, $\left(N^1,N^2\right)\neq(0,0)$.

В противном случае декодирование осуществляется по информации в прямом регистре.

На основании приведенного правила декодирования разработано устройство коррекции стираний для БЧХ-кода с $d_0=6$ (рис. 2), где БРС – блок регистра стираний, БВС – блок вычисления синдрома, БВН – блок вычисления норм, БИА – блок идентификации и анализа, БУКД – блок управления каналами декодирования.

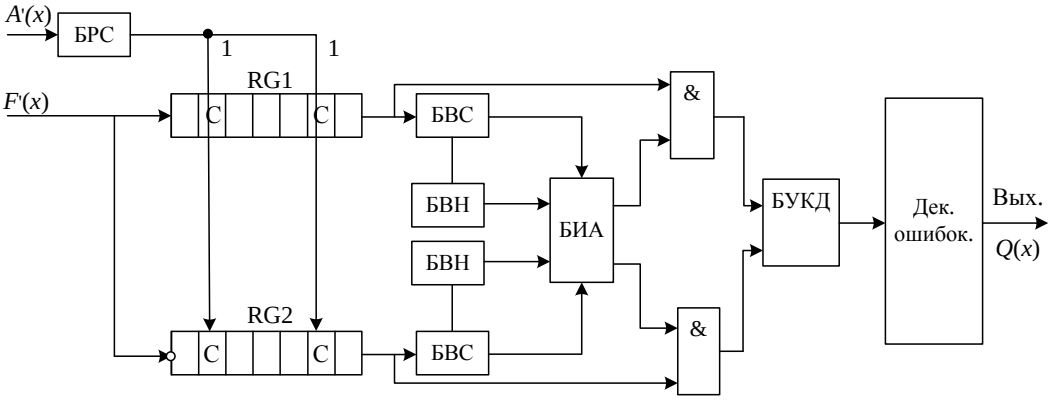


Рис. 2. Декодер стираний с прямым, инверсным каналами и нормами синдромов для БЧХ-кода с $d=6$

Известно [1, 4], что применение норм синдромов для идентификации ошибок позволяет многократно уменьшить количество анализируемых при декодировании синдромов и значительно уменьшить вычислительные затраты на исправление стираний. Аппаратурная сложность устройства исправления (декодера) стираний, основанного на решении систем уравнений предложенного в [2, 3] определяется из выражения:

$$Q = n \cdot 5 \cdot]\log n[+ (5 + \frac{5}{8}) \cdot 5 \cdot 2^5 \cdot]\log n[,$$

где n – длина кодового слова.

Например, при исправлении пятикратных стираний аппаратурная сложность декодера составляет $Q = 5300$. Сложность декодера, рассматриваемого в данной статье, определяется выражением

$$Q_c \approx 2 \cdot n + n \cdot r + 2^{r/2} + \left(C_n^1 + C_n^2\right) + 2^i,$$

где $2 \cdot n$ – сложность регистров хранения прямого и инверсного слов; $2 \cdot n \cdot r$, $2^{r/2}$ – сложность блоков вычисления синдромов и их норм в прямом и инверсном словах, $\left(C_n^1 + C_n^2\right)$ – сложность селектора двухкраных ошибок и 2^i – сложность блока анализа и идентификации, i – число идентификационных параметров.

Таким образом, для приведенного примера исправления пятикратных стираний аппаратурная сложность предложенного декодера равна $Q = 1456$, что примерно в 3,4 раза меньше сложности декодера, предложенного в [2, 3].

Заключение

Для коррекции пятикратных стираний предлагается использовать БЧХ-коды с кодовым расстоянием $d = 6$ для коррекции ошибок с применением норм синдромов и разряда контроля четности в двух каналах декодирования (прямом и инверсном). Установлено, что применение в двух каналах декодеров для исправления двухкратных ошибок при коррекции пятикратных стираний позволяет существенно уменьшить временные затраты по сравнению с известными переборными методами коррекции стираний, и кроме того, уменьшить в более чем три раза аппаратурную сложность по сравнению с устройством коррекции стираний, основанном на решении систем уравнения по нахождению вектора согласования.

EMPLOYMENT SYNDROME NORMS FOR IDENTIFICATION OF MULTIPLICITY OF ERROR, IN ERASURE CORRECTION BY BCH-CODES

N.A. SALAS, V.K. KONOPELKO, A.I. KOROLEV

Abstract

Correction of multiple erasures based on identification of multiplicity of unmatched erased symbols by norm method in two channels (forward and reverse) decoding is examined. It is shown that the use of norm syndromes for the identification of multiplicity of unmatched erasures by BCH codes can effectively and quickly identify their multiplicity for erasures of multiplicity $t_c \le 5$. It is found that the proposed decoding method can reduce more than 3 times the decoding complexity compared to the known method for correcting erasures, based on the solution of systems of equations in Galois fields.

Литература

1. *Конопелько В.К.* Теория прикладного кодирования. Минск, 2004.
2. *Фам Хак Хоан, Конопелько В.К.* // Докл. БГУИР. 2006. №6. С. 19-22.
3. *Фам Хак Хоан, Конопелько В.К.* пат. №3901 U. РБ, МПК (2006).
4. *Липницкий В.А., Конопелько В.К.* Норменное декодирование помехоустойчивых кодов и алгебраические уравнения. Мн., 2007.
5. *Конопелько В.К., Борсикевич А.А. Цветков В.Ю.* Многомерные технологии сжатия, защиты и коммутации изображений. Мн., 2008.

УДК 621.391.14

ИССЛЕДОВАНИЕ ДОСТАТОЧНОГО ЧИСЛА НОРМ СИНДРОМОВ ДЛЯ ДЕКОДИРОВАНИЯ БЧХ-КОДОВ

З.Н. ХОАНГ, В.К. КОНОПЕЛЬКО, Е.Г. МАКЕЙЧИК

Белорусский государственный университет информатики и радиоэлектроники
П. Бровки, 6, Минск, 220013, Беларусь

Поступила в редакцию 2 октября 2012

Рассматривается формирование образующих векторов, нахождение норм синдромов и идентификационных параметров для образующих векторов ошибок кратностей $t = 3 \div 7$ БЧХ-кодов с длиной $n = 127$. Предлагается идентификация на основе совместного использования основных и дополняющих норм. Показывается, что при значении первой компоненты синдрома равной нулю достаточно использовать только дополняющие нормы.

Ключевые слова: синдром *S*, норма синдрома *N*, основные $N_{\text{о}}$, зависимые $N_{\text{з}}$, дополняющие $N_{\text{д}}$ нормы, кратность ошибок *t*, длина кода *n*, образующие вектора ошибок.

Введения

Нормы синдромов эффективно используются в обработке БЧХ-кодов для коррекции ошибок кратностей $t = 1 \div 3$ [1, 2]. Однако их применение для контроля ошибок большой кратности $t > 3$ не исследовалось из-за сложности анализа, синтеза формирования множества образующих ошибок, поиска идентификационных параметров. Ниже приводятся исследования по изучению норм синдромов в обработке кодов длины $n = 127$, исправляющих ошибки кратности $3 \le t \le 7$, их сравнение с БЧХ-кодами для $n = 31$.

Алгоритм нахождения норм синдромов БЧХ-кодов и идентификаторов, образующих векторов ошибок

Для нахождения норм синдромов и идентификаторов, образующих векторов ошибок, приведен вычислительный эксперимент, который включает следующие этапы: формирование образующих векторов ошибок, вычисление синдромов и их норм, их различия для образующих векторов ошибок и формирование отличающихся множеств норм $\{N_1, N_2, ...N_i...\}$, обозначающих все образующие вектора ошибок. На рис. 1 приведен алгоритм вычисления норм и идентификаторов, который можно использовать для любых кратностей ошибок t и длины кодов n.

При реализации алгоритмов формирования образующих векторов, вычисления синдрома и их норм, а также поиска идентификаторов использовались система с интерпретируемым функциональным языком программирования Mathematica, а программа разрабатывалась в среде операционной системы Window 7 для 4-ядерного процессора Intel Core i7.

Среднее время проведения вычислительных экспериментов в зависимости от кратностей корректируемых ошибок t и длины кодов n представлено в табл. 1.

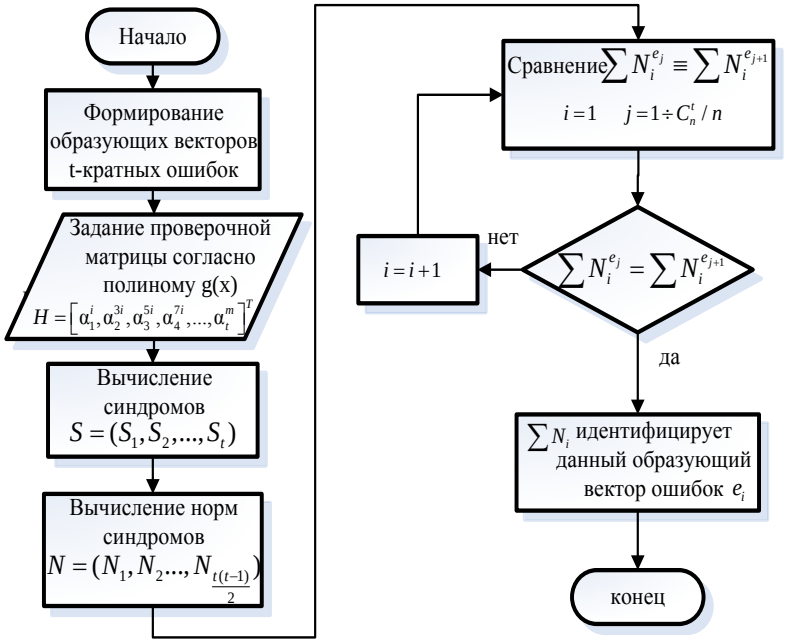


Рис. 1. Алгоритм вычисления норм и нахождения идентификационных параметров образующих векторов ошибок

Таблица 1. **Зависимость среднего времени проведения вычислительных экспериментов для поиска идентификационных параметров от кратности t**

Кратность ошибок t / Длина кода n	2	3	4	5	6	7
31	менее 1 с	менее 1 с	2-3 с	30-35 с	2-3 мин	9-10 мин
127	менее 1 с	18-20 с	8-10 мин	3-4 ч	около 70 ч	более 90 суток

Анализ данных табл. 1 показывает, что с ростом длины кода n и кратности корректируемых ошибок t, среднее время проведения вычислительного эксперимента резко возрастает. Например, при кратности ошибок $t=6$ для кодов с $n=31,127$ среднее время составляет 2-3 м и около 70 ч соответственно. Причем время, затрачиваемое на формирование образующих векторов ошибок, значительно меньше времени, затрачиваемого на вычисление синдромов, их норм и нахождение идентификаторов образующих векторов ошибок (для формирования образующих векторов шестикратных ошибок для $n=127$ требуется только 20-30 м, а для вычисления синдромов, их норм и нахождения идентификаторов уже около 70 ч).

Идентификационные параметры для БЧХ-кодов длиной 127

В [1, 2] установлено, что число используемых норм зависит от числа образующих векторов ошибок. Как показано в [3] для длины $n=31$ все нормы N можно разбить на две группы: основные $N_{\text{о}}$ и зависимые $N_{\text{з}}$. В общем случае для идентификации образующих векторов ошибок достаточно использовать основные нормы $N_{\text{о}}$. Однако поскольку некоторые синдромы $S_i=0$, то для них основные $N_{\text{о}}$ нормы не вычисляются, а оставшихся недостаточно для идентификации образующих векторов ошибок, что приводит к необходимости использовать зависимые нормы $N_{\text{з}}$ наряду с основными $N_{\text{о}}$. Это приводит при больших t к числу норм большему, чем число синдромов. В табл. 2-4 приведены результаты вычислительного эксперимента по поиску идентификационных параметров из множеств основных $N_{\text{о}}$ и зависимых $N_{\text{з}}$ норм, позволяющих идентифицировать соответствующие образующие вектора ошибок, где дополняющие нормы $N_{\text{д}}$ выбираются из числа зависимых $N_{\text{з}}$.

Таблица 2. **Зависимость числа образующих векторов ошибок, основных N_o и дополняющих $N_д$ норм достаточных для идентификации образующих векторов ошибок от кратности ошибок при одной компоненте синдрома $S_i = 0$, $n = 127$**

Синдром S_i / Кратность t	Число образующих векторов ошибок (1) / Идентификационные параметры (2)	$S_i = 0$	$S_1 = 0$	$S_2 = 0$
3	(1)	2562	21	21
	(2)	N_1, N_2	N_3	N_2
4	(1)	78780	644	644
	(2)	N_1, N_2, N_3	N_4, N_5	N_2, N_3
5	(1)	1924825	15155	15155
	(2)	N_1, N_2, N_3, N_4	N_5, N_6, N_7	N_2, N_3, N_4
6	(1)	38835778	305004	305004
	(2)	N_1, N_2, N_3, N_4, N_5	N_6, N_7, N_8, N_9	N_2, N_3, N_4, N_5
Синдром S_i / Кратность t	Число образующих векторов ошибок (1) / Идентификационные параметры (2)	$S_4 = 0$	$S_5 = 0$	$S_6 = 0$
3	(1)			
	(2)			
4	(1)	630		
	(2)	N_1, N_2		
5	(1)	15155	151225	
	(2)	N_1, N_2, N_4	N_1, N_2, N_3	
6	(1)	305067	305032	305053
	(2)	N_1, N_2, N_4, N_5	N_1, N_2, N_3, N_5	N_1, N_2, N_3, N_4

Таблица 3. **Зависимость числа образующих векторов ошибок, основных N_o и дополняющих $N_д$ норм, достаточных для идентификации образующих векторов ошибок от кратности ошибок t при двух компонентах синдрома $S_i = S_j = 0$, $n = 127$**

Синдром $S_{i,j} = 0$ / Кратность t	Число образующих векторов ошибок (1) / Идентификационные параметры (2)	$S_1 = 0$ $S_2 = 0$	$S_1 = 0$ $S_3 = 0$	$S_1 = 0$ $S_4 = 0$	$S_1 = 0$ $S_5 = 0$	$S_1 = 0$ $S_6 = 0$	$S_2 = 0$ $S_3 = 0$	$S_2 = 0$ $S_4 = 0$	$S_2 = 0$ $S_5 = 0$
5	(1)			7				7	
	(2)			N_6				N_2	
6	(1)	2541	2548	2478	2513	2499	2499	2499	2527
	(2)	N_9, N_{10}	N_7, N_8	N_6, N_8	N_6, N_7	N_6, N_7	N_3, N_4	N_2, N_4	N_2, N_3
Синдром $S_{i,j} = 0$ / Кратность t	Число образующих векторов ошибок (1) / Идентификационные параметры (2)	$S_2 = 0$ $S_6 = 0$	$S_3 = 0$ $S_4 = 0$	$S_3 = 0$ $S_5 = 0$	$S_3 = 0$ $S_6 = 0$	$S_4 = 0$ $S_5 = 0$	$S_4 = 0$ $S_6 = 0$	$S_5 = 0$ $S_6 = 0$	
5	(1)		7						
	(2)		N_1						
6	(1)	2485	2478	2506	2492	2462	2485	2485	
	(2)	N_2, N_3	N_1, N_4	N_1, N_3	N_1, N_4	N_1, N_2	N_1, N_2	N_1, N_2	

Таблица 4. **Зависимость числа образующих векторов ошибок, основных N_o и дополняющих $N_д$ норм достаточных для идентификации образующих векторов ошибок, от кратности ошибок t при трех компонентах синдрома $S_i = S_j = S_z = 0$, $n = 127$**

Синдром $S_{i,j,z}=0$ / Кратность t	Число образующих векторов ошибок (1) / Идентификационные параметры (2)	$S_1=0$ $S_2=0$ $S_4=0$	$S_1=0$ $S_3=0$ $S_4=0$	$S_1=0$ $S_4=0$ $S_5=0$	$S_1=0$ $S_4=0$ $S_6=0$	$S_1=0$ $S_5=0$ $S_6=0$	$S_2=0$ $S_3=0$ $S_4=0$	$S_2=0$ $S_3=0$ $S_6=0$
6	(1)	21	14	21	35	28	21	42
	(2)	N_{10}	N_7	N_6	N_6	N_6	N_4	N_3
Синдром $S_{i,j,z}=0$ / Кратность t	Число образующих векторов ошибок (1) / Идентификационные параметры (2)	$S_1=0$ $S_4=0$ $S_5=0$	$S_2=0$ $S_4=0$ $S_6=0$	$S_2=0$ $S_5=0$ $S_6=0$	$S_3=0$ $S_4=0$ $S_5=0$	$S_3=0$ $S_4=0$ $S_6=0$	$S_3=0$ $S_5=0$ $S_4=0$	$S_4=0$ $S_5=0$ $S_6=0$
6	(1)	14	14	21	42	14	14	21
	(2)	N_2	N_2	N_2	N_1	N_1	N_1	N_1

Анализ табл. 2-4, показывает, что число используемых норм в два раза меньше числа норм, предложенных в [1, 2]: это приводит к уменьшению в два раза числа входов селектора декодера. На рис. 2 представлена зависимость достаточного числа норм N для идентификации ошибок кратности t для БЧХ-кодов длиной $n = 31{,}127$.

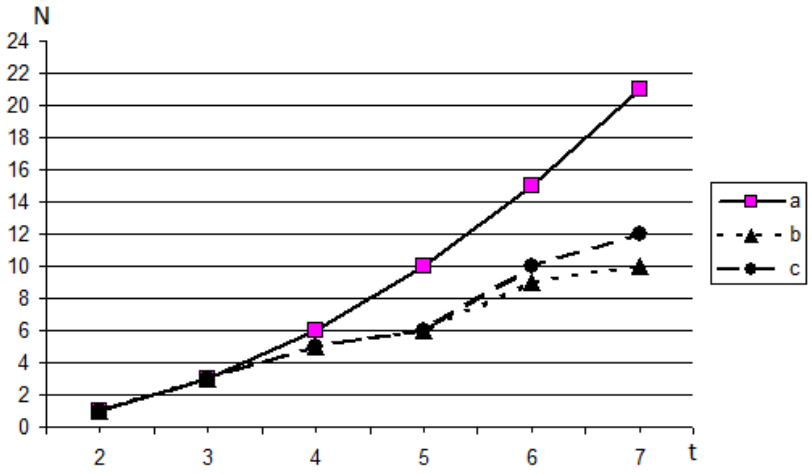


Рис. 2. Зависимость достаточного числа норм N от кратности ошибок t: a – число норм из [1, 2]; b – число норм для $n = 31$; c – число норм для $n = 127$

Анализ зависимостей на рис. 2 показывает, что количество идентификационных параметров для БЧХ-кода с $n = 127$ незначительно больше, чем для БЧХ-кода с $n = 31$. Кроме того, видно, что декодирующее устройство для коррекции больших кратностей ошибок t на большей длине кода n может быть реализовано. Например, для построения блока идентификатора шестикратных ошибок можно использовать ПЗУ емкостью 647 Мб, в котором хранятся 40703775 образующих векторов ошибок. Блок идентификатора также может быть построен и на ПЛИС, емкость которой должна быть не менее 40703775 элементов «И». Такое количество логических элементов обеспечивает ПЛИС Spartan 3 XC3S4000, у которой имеется 6912 конфигурируемых логических блоков, каждый из которых состоит из 62208 логических элементов.

Анализ данных табл. 2-4 также показывает, что для идентификации ошибок кратностей $3 \le t \le 7$ при $n = 127$ исключить какую либо подматрицу с $\alpha^{(2m+1)i}$ в проверочной матрице H БЧХ-кода нельзя (хотя это имеет место в кодах с $n = 31$). Поэтому параметры БЧХ-кодов, задаваемых проверочной матрицей $H = \left[\alpha_1^i, \alpha_2^{3i}, \alpha_3^{5i}, \alpha_4^{7i}, ..., \alpha_t^m\right]^T$, равны $(127{,}106)$, $(127{,}99)$, $(127{,}92)$, $(127{,}106)$, $(127{,}78)$ для $t = 3;4;5;6;7$ соответственно. Однако, как отмечено в [4], эти коды представляют собой «хорошие коды» с малой избыточностью.

Из данных табл. 2-4 следует, что если отказаться от декодирования образующих векторов ошибок, для которых синдром $S_1 = 0$ (в этом случае для идентификации ошибок используются только основные нормы N_o), то число отказов от декодирования ошибок кратности $t = 3;4;5;6$ на длине кода $n = 127$ равно 0,8%, 0,8%, 0,78%, 0,78% соответственно, (это примерно в 4 раза меньше по сравнению при аналогичном отказе от декодирования БЧХ-кодов с $n = 31$ [3]). Проведенный эксперимент для кодов длиной $n = 511$ показал, что число отказов от декодирования уменьшается до 0,2%. Это позволяет уменьшить в более чем два раза число входов у селектора декодирующего устройства при небольшом числе отказов от декодирования при коррекции ошибок кратности $t = 6$.

Заключение

Показано, что среднее время проведения вычислительного эксперимента по формированию образующих векторов ошибок, вычислению синдромов, норм и нахождению идентификаторов резко возрастает с увеличением длин кодов и числа корректируемых ошибок, а число используемых норм для БЧХ-кодов с различными длинами приблизительно одинаково и в два раза меньше числа норм, предложенных в [1, 2]. Также установлено, что с ростом длин кодов имеется возможность отказаться от декодирования векторов ошибок, для которых синдром $S_1 = 0$, поскольку число соответствующих образующих векторов ошибок менее одного процента. Все это приводит к пятикратному уменьшению числа входов блока идентификации при коррекции шестикратных ошибок.

ANALYSIS OF A SUFFICIENT NUMBER OF NORMS SYNDROMES DECODING BCH-CODES

D.N. HOANG, V.K. KONOPELKO, E.G. MAKEICHIK

Abstract

The formation of generating vectors, the calculus of syndrome norms and the identification parameters for generating error vectors of multiplicities $n = 127$ for BCH-codes with length $n = 31$ are studied. Identification based on the sharing use of main and complementaries norms in case of null value of the first components of the syndrome is proposed.

Литература

1. *Конопелько В.К., Липницкий В.А.* Теория норм синдромов и перестановочное декодирование помехоустойчивых кодов. Минск, 2004.
2. *Липницкий В.А., Конопелько В.К.* Норменное декодирование помехоустойчивых кодов и алгебраические уравнения. Минск, 2007.
3. *Конопелько В.К., Хоанг Н.З.* // Докл. БГУИР. 2012. №8. С. 70-75.
4. *Мак-Вильяме Ф.Дж.* Теория кодов, исправляющих ошибки. М., 1979.

УДК 517.9

СЕТЕВОЕ КОДИРОВАНИЕ НА ОСНОВЕ ИСПОЛЬЗОВАНИЯ ВЕЙВЛЕТ-ПРЕОБРАЗОВАНИЙ НАД КОНЕЧНЫМИ ПОЛЯМИ

А.А. ОХРИМЕНКО, С.Б. САЛОМАТИН

Белорусский государственный университет информатики и радиоэлектроники
П. Бровки, 6, Минск, 220013, Беларусь

Поступила в редакцию 3 сентября 2012

Рассматривается метод сетевого кодирования группового сигнала на основе применения вейлет преобразований над конечными полями. Показана возможность применения дискретных вейвлет-преобразований Хаара и Добеши, формируемых над конечными полями, для кодирования и декодирования информации в сетевой структуре.

Ключевые слова: сетевой код, конечное поле, дискретное вейвлет-преобразование.

Модель системы сетевого кодирования

Рассмотрим канал сети, состоящий из нескольких элементов сети N_1, N_2, …, N_L, которые обмениваются между собой информацией через промежуточный, ретрансляционный элемент сети N_R. Промежуточный узел запоминает в буферной памяти пакеты, поступившие по входным линиям, образует их линейные комбинации, а затем рассылает их копии по тем своим выходным линиям, которые могут через другие узлы доставить их получателям [1-3].

Предполагается, что элементы сети поддерживают режим полудуплексного взаимодействия. Имеются две фазы взаимодействия элементов сети в канале. В первой фазе элементы N_1, …, N_L передают пакеты $\{X_i, i=1,...L\}$ на элемент N_R, который принимает сигнал

$$y_R = \sum_{i=1}^{L} h_{i,R} x_i + v_R,\ x_i \in X_i, \qquad (1)$$

где $h_{i,j}$ – комплексный коэффициент, характеризующий свойства канала; v_3 – комплексный, гауссовский, внутренний шум с нулевым математическим ожиданием и единичной дисперсией принимающей части элемента сети N_R.

Предполагается нормализация мощности и синхронизация сигналов передаваемых пакетов. Также предполагается возможность оценки коэффициентов $h_{i,j}$ для каждого элемента сети.

Во второй фазе элемент сети N_R формирует на основе принятых сообщений пакет X_R, сигнал которого x_R в широковещательном формате передается на элементы сети. Последние принимают сигналы

$$y_1 = h_{R,1} x_R + v_1,\ \ldots,\ y_L = h_{R,L} x_L + v_L, \qquad (2)$$

где $x_R = f(x_1,...x_L)$ является функцией от $\{x_i, i=1,...,L\}$.

Кодирование $f(x_1, ..., x_L)$ может быть выполнено различными способами [1-2].

Помехоустойчивые методы кодирования используют ортогональные сигналы. Для сетевых структур важным аспектом является разнообразие массивов ортогональных сигналов и преобразований.

Вейвлет-преобразования над конечными полями

Вейвлет-функции могут быть определены над конечными полями $GF(q)$. Базисная (материнская) вейвлет-функция над конечным полем (ВФКП) представляется в виде N-мерного вектора [4]:

$$\boldsymbol{\psi}_{1,0} = (\psi_{1,0}(0), \psi_{1,0}(1), ..., \psi_{1,0}(N-1)), \quad (3)$$

где каждая компонента ψ принадлежит расширенному полю $GF(p^s)$, p – простое число, s – целое положительное число.

Рассмотрим вначале случай простого поля $GF(p)$. Пусть N будет целым и $D(N)$ – дивизор, который объединяет множество делителей N. Структура конечного поля не позволяет выполнить такую же операцию масштабирования (шкалирования), какая производится для непрерывных вейвлет-функций в поле действительных чисел. Операцию масштабирования в конечном поле выполняет дивизор длины.

Введем следующие операции.

1. Операция шкалирования $\boldsymbol{\psi}_{j,0}$, где

$$\psi_{j,0}(i) = \psi_{1,0}(ji) \quad \forall j \in D(N/2) := \{ j \text{ таких, что } j \mid N/2 \}. \quad (4)$$

2. Операция сдвига $\boldsymbol{\psi}_{j,k}$:

$$\psi_{j,k}(i) = \psi_{j,0}(i + \frac{Nk \bmod N}{j}), \ \forall k = 0,1,...,N-1. \quad (5)$$

Вейвлет-функция может быть записана в виде

$$\boldsymbol{\psi}_{j,k} = (\psi_{j,k}(0), \psi_{j,k}(1), \psi_{j,k}(2), ..., \psi_{j,k}(N-1)), \quad (6)$$

где масштабирование и/или сдвиг выполняются по версии базисной ВФКП.

Свойство. ВФКП $\boldsymbol{\psi}_{j,k}$ подчиняются соотношению

$$\sum_{i=0}^{N-1} \boldsymbol{\psi}_{j,k}(i) \equiv 0 \bmod p, \ (\forall j,k). \quad (7)$$

Вейвлет-преобразование над конечным полем. Пусть задан вектор-сигнал $\mathbf{v} = (v_0, v_1, \ldots, v_{N-1})$ длины N над полем $GF(p)$ характеристики $p \neq 2$ и вейвлет-функции $\boldsymbol{\psi}_{j,k}$ над полем $GF(p^s)$.

Вейвлет-преобразование над конечным полем (ВПКП) сигнала $\mathbf{v}$ определяется как

$$\Psi_F(j,k) \equiv \sum_{i=0}^{N-1} v_i \psi_{j,k}(i) \bmod p = < \mathbf{v}, \boldsymbol{\psi}_{j,k} >. \quad (8)$$

Преобразование Хаара над конечным полем. Базис Хаара в конечных полях можно записать следующим образом:

$$\psi_{1,0}(i) = \begin{cases} 1, & \text{если } 0 \le \dfrac{i}{N} < \dfrac{1}{2} \\ p-1, & \text{если } \dfrac{1}{2} \le \dfrac{i}{N} < 1 \\ 0, & \text{в остальных случаях} \end{cases} \quad (9)$$

или в форме

$$\psi_{j,0}(i) = \begin{cases} (p-1)^{\left\lfloor \frac{i \bmod N}{N/2} \right\rfloor}, & \text{если } 0 \le \dfrac{i}{N} < 1 \\ 0, & \text{в остальных случаях} \end{cases}. \quad (10)$$

Пример. Предположим, требуется построить функции Хаара длиной $N = 8$ над конечным полем $GF(p)$. Возможные коэффициенты масштабирования $j \in D(4) = \{1,2,4\}$. Воспользовавшись вышеприведенной формулой, получаем:

$j = 1 \to \boldsymbol{\psi}_{1,0} = (1,1,1,1, p-1, p-1, p-1, p-1)$,

$j = 2 \to \boldsymbol{\psi}_{2,0} = (1,1, p-1, p-1, p-1, 0, 0, 0, 0)$,

$j = 4 \to \boldsymbol{\psi}_{4,0} = (1, p-1, 0, 0, 0, 0, 0, 0)$.

Полученные функции удовлетворяют операции сдвига. Так, функция $\boldsymbol{\psi}_{2,0}$ после сдвига образует вектор

$\boldsymbol{\psi}_{2,1} = (0,0,0,0,1,1, p-1, p-1)$.

Свойство. Исходная версия функции $\boldsymbol{\psi}_{j,0}$ позволяет получить j различных сдвигов функции $\boldsymbol{\psi}_{j,k}$.

Нормализация энергии. Поскольку N является степенью двойки и j принадлежит $D(N/2)$, то (N/j) также степень двойки. Предположим теперь, что $p \equiv \pm 1 \bmod 8$, тогда $\sqrt{N/j} \in GF(p)$. Тогда нормализованное преобразование может быть записано как

$$V_{FW}(j,k) = \frac{1}{\sqrt{(N/j) \bmod p}} \sum_{i=0}^{N-1} v_i \psi_{j,k}(i) \bmod p. \qquad (11)$$

Определим подмножество $S \subseteq D(N/2)$ такое, что

$$\sum_{j \in S \subseteq D(N/2)} j = N - 1. \qquad (12)$$

Положим $N = 2^m$, тогда $D(N/2)=\{1, 2, 4, 8, \ldots, 2^{m-1}\}$ и $\sum_{j \in D(n/2)} j = \sum_{j=1}^{m-1} 2^j = N - 1$. В этом случае $j \in D(N/2)$ и все значения индекса j могут быть использованы для построения базисных вейвлетов. Построенные таким образом функции вместе с последовательностью из всех единиц (1, 1, …, 1) образуют ортогональное множество N сигналов над полем $GF(p)$ или, другими словами, ортогональный базис Хаара.

Пример. Над полем $GF(7)$ ВФКП Хаара и нормализованные ВФКП Хаара имеют вид

(1 1 1 1 1 1 1 1)	(1 1 1 1 1 1 1 1)
(1 1 1 1 6 6 6 6)	(6 6 6 6 1 1 1 1)
(1 1 6 6 0 0 0 0)	(4 4 3 3 0 0 0 0)
(0 0 0 0 1 1 6 6)	(0 0 0 0 4 4 3 3)
(1 6 0 0 0 0 0 0)’	(5 2 0 0 0 0 0 0)
(0 0 1 6 0 0 0 0)	(0 0 5 2 0 0 0 0)
(0 0 0 0 1 6 0 0)	(0 0 0 0 5 2 0 0)
(0 0 0 0 0 0 1 6)	(0 0 0 0 0 0 5 2)

Для построенных функций справедливы следующие соотношения:

$\sum_{i=0}^{N-1} \psi_{j,k}(i) \equiv 0 \bmod p$, $\sum_{i=0}^{N=1} \psi_{j,k}^2(i) \equiv 1 \bmod p$,

$\sum_{i=0}^{N-1} \psi_{j,k}(i) \psi_{j',k'}(i) \equiv 0 \bmod p, \forall j \neq j'$ или $k \neq k'$.

Если N не является степенью двойки, то могут быть вычислены не ортогональные вейвлет-функции. Например, если $N = 24$, то над полем $GF(7)$ получаем следующее множество сдвигов $D(12) = \{1, 2, 3, 4, 6, 12\}$. Вейвлет-функции имеют вид

Число возможных сдвигов

$j = 1$	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	1
$j = 2$	1 1 1 1 1 1 1 1 1 1 1 1 6 6 6 6 6 6 6 6 6 6 6 6	1
$j = 6$	1 1 1 6 6 6 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	4
$j = 12$	1 1 6 6 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	6
	1 6 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	12

Полученные сигналы не образуют ортогонального множества, так, например, $\langle \boldsymbol{\psi}(2,1), \boldsymbol{\psi}(6,0) \rangle \neq 0 \bmod p$.

Структура вейвлет-функции Хаара над конечным полем позволяет строить пирамидально-фильтровые алгоритмы.

Пример. Двухэлементные фильтры (1, 1) для преобразования Хаара над полем $GF(7)$ имеют следующие импульсные характеристики:

$h = [5, 5]$, $h^*[5, 5]$; $g = [2, 5]$, $g^* = [5, 2]$.

Вейвлет-функции Добеши над простыми конечными полями. Рассмотрим стандартную постановку задачи Добеши построения ортогональных вейвлет-функций. Функция прототип имеет вид

$$\psi_{j,k}(i) = \left(\sqrt{2}\right)^j \psi\left(2^j i - k\right). \tag{13}$$

Анализ с разным разрешением использует масштабные функции. В нашем случае в качестве масштабных функций можно определить такие функции φ, которые удовлетворяют сравнению

$$\varphi_{j,k}(i) \equiv \left(2\right)^{j/2} \varphi(2^j i - k), \tag{14}$$

причем выполняется условие $\varphi_{j,k}(i) \equiv \sqrt{2}\varphi(2i - k) \bmod p$.

Дискретный вейвлет-анализ использует понятие зеркальных квадратурных фильтров с импульсными характеристиками, соответственно $\mathbf{h} = (h_0, h_{1,}\ldots, h_{N-1})$ и $\mathbf{g} = (g_0, g_{1,}\ldots, g_{N-1})$. Применим такой подход при решении нашей задачи. Уравнения, обеспечивающие детализацию спектра, с использованием импульсных характеристик квадратурных зеркальных фильтров $\mathbf{h}$ можно записать как

$$\varphi(i) \equiv \sqrt{2} (\bmod p) \sum_{k=0}^{N-1} h_k \varphi(2i - k) \bmod p. \tag{15}$$

Соответственно, вейвлет-функции используют альтернативный фильтр $\mathbf{g}$ следующим образом:

$$\psi(i) \equiv \sqrt{2} (\bmod p) \sum_{k=0}^{N-1} g_k \varphi(2i - k) \bmod p. \tag{16}$$

Импульсные характеристики фильтров определяются из соотношений

$$\sum_{k=0}^{N-1} h_k \equiv \sqrt{2} \bmod p,\ \sum_{k=0}^{N-1} g_k \equiv 0 \bmod p,\ g_k \equiv (-1)^k h_{N-1+k} \bmod p,\ \sum_{k=0}^{N-1} h_k h_{k+2m} \equiv 0 \bmod p, m \neq 0. \tag{17}$$

Пример. Построим фильтры для вейвлет-функций Добеши конечного поля *GF*(97), $N = 4$.

Квадратурные зеркальные фильтры определяются как

- сглаживающий (нижних частот) фильтр **h** = [92, 47, 12, 57];
- детализирующий (высоких частот) фильтр **g** =[57, 85, 47, 5].

Значения импульсных характеристик фильтров связаны соотношениями

$g_k \equiv (-1)^k h_{3-k} \mod 97$, $\sum_{k=0}^{3} h_k \equiv 14 \mod 97$, $14^2 = 196 \equiv 2 \mod 97$;

$\sum_{k=0}^{3} g_k \equiv 0 \mod 97$, и $\sum_{k=0}^{3} h_k h_{k+2} \equiv 0 \mod 97$.

Синтез сложных сигналов на основе вейвлет-функций Хаара конечных полей

Ортогональные вейвлет-функции конечного поля можно использовать для формирования сигналов при сетевом кодировании. В таких системах каждый элемент сети использует для передачи информации свой сигнал – кодовую последовательность. В качестве таких кодовых последовательностей можно предложить использовать сигналы, которые получаются путем масштабирования/сдвига базисного вейвлета.

Рассмотрим пример кодирования сигналов для N=8 и поля *GF*(7).

Оператор суммы в y_R выполняет операцию векторного суммирования по mod p. Информационный сигнал в каждом канале состоит из N одинаковых символов, которые смешиваются с канальной вейвлет-функцией. Например, пусть для третьего канала информационный символ равен 2, а канальная вейвлет-функция имеет вид $\boldsymbol{\psi}_{2,0}$ = (4 4 3 3 0 0 0 0). Тогда канальный сигнал имеет вид

(2 2 2 2 2 2 2 2) $\otimes$ (4 4 3 3 0 0 0 0) = (1 1 6 6 0 0 0 0) mod 7

или в сокращенной записи

$2^{(8)} \otimes 4^{(2)}3^{(2)}0^{(4)} = 1^{(2)}6^{(2)}0^{(4)} \mod 7$.

Теперь рассмотрим случай, когда информация передается сразу по всем 8 каналам. Пусть информационный вектор **a** = [3, 0, 2, 1, 6, 5, 5, 4]^T. Вектор опорных вейвлет-функций имеет вид [$\boldsymbol{\psi}_{0,0}$, $\boldsymbol{\psi}_{1,0}$, $\boldsymbol{\psi}_{2,0}$, $\boldsymbol{\psi}_{2,1}$, $\boldsymbol{\psi}_{4,0}$, $\boldsymbol{\psi}_{4,1}$, $\boldsymbol{\psi}_{4,2}$, $\boldsymbol{\psi}_{4,3}$]. После перемножения в каналах символов информационных и вейвлет-последовательностей, на входе сумматора Σ получим

$\mathbf{r} = 3^{(8)} \oplus 0^{(8)} \oplus 1^{(2)}6^{(2)}0^{(4)} \oplus 0^{(4)}4^{(2)}3^{(2)} \oplus 2^{(1)}5^{(1)}0^{(6)} \oplus 0^{(2)}4^{(1)}3^{(1)}0^{(4)} \oplus 0^{(4)}4^{(1)}3^{(1)}0^{(2)} \oplus 0^{(6)}6^{(1)}1^{(1)} \equiv$

$\equiv$ (6, 2, 6, 5, 4, 3, 5, 0) mod 7.

Так как вейвлет-функции ортогональны, то на приемной стороне информация однозначно выделяется с помощью операции скалярного произведения векторов над конечным полем *GF*(p):

- канал 3 $\rightarrow$ < **r**, $\boldsymbol{\psi}_{2,0}$ > $\equiv$ 2 mod 7;
- канал 8 $\rightarrow$ < **r**, $\boldsymbol{\psi}_{4,3}$ > $\equiv$ 4 mod 7, и т.д.

Заключение

Описаны методы построения дискретных вейвлет-преобразований в конечных полях и модулярных вычислениях. Показаны перспективы использования рассмотренных преобразований для решения задач сетевого кодирования.

NETWORK CODING ON THE USE OF WAVELET TRANSFORM IN FINITE FIELDS

A.A. OKHRIMENKO, S.B. SALOMATIN

Abstract

A method of network coding based on the use of wavelet transform in finite fields is presented. Algorithms of wavelet transforms Haar and Daubechies in finite fields for network coding has been considered.

Литература

1. *Габидулин Э.М., Пилипчук Н.И., Колыбельников А.И. и др*. // Сетевое кодирование. ТРУДЫ МФТИ. 2009. Т. 1, №2. С. 3-28.
2. Physical layer network coding [Электронный ресурс]. Режим доступа: http://arxiv.org/ftp/arxiv/papers/0704/0704.2475.pdf
3. *Li Y.R., Yeung R.W., Cai N.* // IEEE Trans. on Inform. 2003. Vol. 49 (2). P. 371-381.
4. *Фрейзер М.* Введение в вейвлеты в свете линейной алгебры. М., 2008.

УДК 621.391.25

ОБНАРУЖЕНИЕ СКРЫТНО ДВИЖУЩИХСЯ ОБЪЕКТОВ

А.И. МИТЮХИН

Институт информационных технологий
Козлова, 28, Минск, 220037, Беларусь

Поступила в редакцию 12 июня 2012

Рассматривается задача обнаружения по изображениям скрытно движущегося объекта. При этом требуется произвести оценку скорости движения объекта, направления его движения, пройденного расстояния. Исследуется возможность обнаружения динамических изображений в частотной области с помощью дискретного преобразования Хартли (ДПХ).

Ключевые слова: пиксел, обнаружение объекта, базис Хартли, спектр последовательности, скорость объекта, шум.

Введение

В ряде приложений требуются знания текущих координат объекта, скорости его движения, направления движения, пройденного объектом расстояния. Например, при обнаружении скрытно движущейся военной техники, дистанционном зондировании земной поверхности с целью метеорологических наблюдений и др. Искажение изображения помехами приводит к ошибкам измерения координат, параметров движения. Предлагается обнаружение объектов динамических изображений осуществлять в частотной области с помощью дискретного преобразования Хартли (ДПХ). В отличие от алгоритма избыточного комплексного дискретного преобразования Фурье (ДПФ), преобразование Хартли относится к действительным преобразованиям и поэтому вычислительно более простое.

Алгоритм обнаружения движущегося объекта

Изменяющиеся во времени изображение можно представить в виде дискретной трехмерной функции $g_{x,y,t}$. Пусть имеется последовательность из K изображений $g_{x,y,t}$ с пространственными дискретными переменными (x, y) по оси x и по оси y двумерного евклидового пространства. Будем предполагать, что обнаруживаются изменения изображений $g_{x,y,t}$ в последовательности кадров в моменты времени $t = 0,1,\ldots,i,\ldots,K-1$. Изменения сцен изображений g_{x,y,t_i} и g_{x,y,t_j} свидетельствуют о наличии движущихся объектов. Каждое пространственное изображение отображается матрицей данных размером $M \times N$. Алгоритм обнаружения объекта основывается на дискретном преобразовании Хартли [1]. Базис Хартли выражается векторами с действительными компонентами:

$$\boldsymbol{h}_v = \left[\operatorname{cas}\left(\frac{2\pi}{N}0v\right), \operatorname{cas}\left(\frac{2\pi}{N}1v\right), \operatorname{cas}\left(\frac{2\pi}{N}2v\right), \ldots, \operatorname{cas}\left(\frac{2\pi}{N}(N-1)v\right) \right]^T,$$

где $\operatorname{cas}\left(\frac{2\pi}{N}v\right) \equiv \cos\left(\frac{2\pi}{N}v\right) + \sin\left(\frac{2\pi}{N}v\right), \forall v \in \mathbb{Z}^+, 0 \le v \le N-1;$

$$\boldsymbol{h}_u = [\mathrm{cas}\left(\frac{2\pi}{N}0u\right), \mathrm{cas}\left(\frac{2\pi}{N}1u\right), \mathrm{cas}\left(\frac{2\pi}{N}2u\right), \ldots, \mathrm{cas}\left(\frac{2\pi}{N}(N-1)u\right)],$$

где $\mathrm{cas}\left(\frac{2\pi}{M}u\right) \equiv \cos\left(\frac{2\pi}{M}u\right) + \sin\left(\frac{2\pi}{M}v\right), \forall u \in \mathbb{Z}^+, 0 \le v \le M-1.$

Последовательность из K изображений можно представить в виде суммы проекций изображений каждого кадра на горизонтальную и вертикальную оси (x и y). Обработке подвергаются дискретные отсчеты проекций изображения, представляющие собой положительные действительные числа. В поле действительных значений отсчетов $g_n, \left(\forall n \in \mathbb{Z}^+, 0 \le n \le N-1\right)$, вектор $\boldsymbol{g} = [g_0, g_1, \ldots, g_{N-1}]^T$ отображается посредством ДПХ в вещественный вектор

$\hat{\boldsymbol{g}} = \left[\hat{g}_0, \hat{g}_1, \ldots, \hat{g}_{N-1}\right]^T$,

где элементы вектора $\hat{g}_v$ определяются равенством

$$\hat{g}_v = \frac{1}{N}\sum_{n=0}^{N-1} g_n \mathrm{cas}\left(\frac{2\pi v n}{N}\right). \qquad (1)$$

Пусть интересующий объект отображается одним пикселом. Проекции изображений каждого кадра на ось x выразим линейной комбинацией дискретных последовательностей множества $\{h_x\} = \left\{\mathrm{cas}\left(\frac{2\pi x}{N}\right)\right\}$. Так как анализ изображений проводится по всем K последовательным кадрам, в результате получается одномерная K-точечная последовательность $g_x(t)$, определяемая следующим соотношением:

$$g_x(t) = \sum_{x=0}^{N-1}\sum_{y=0}^{M-1} g_{x,y,t}\,\mathrm{cas}\left(\frac{2\pi x}{N}\right), t = 0,1,\ldots,K-1. \qquad (2)$$

Если объект за время между первым и вторым кадром сдвигается на один пиксел по оси x, сумма (2) равна вещественному значению отсчета h_1 последовательности h_x. Сдвигу изображения за временной интервал между двумя кадрами на i пикселов по оси x соответствует значение отсчета h_i последовательности h_x. Так как функции $\mathrm{cas}\left(\frac{2\pi v}{N}\right)$ удовлетворяют свойству периодичности

$$\mathrm{cas}\left(\frac{2\pi(v+Nl)}{N}\right) = \mathrm{cas}\left(\frac{2\pi v}{N}\right), \forall l \in \mathbb{Z},$$

при постоянном сдвиге равном i в момент времени $t = K-1$ сформируется последовательность с номером i множества $\{h_x\}$. По мере увеличения i возрастает соответствующая частота v функции Хартли. Величина сдвига i будет пропорциональна составляющей скорости движения объекта в пикселах на кадр по оси x. Таким образом, для вычисления составляющей скорости по оси x следует найти значение v. Для решения этой задачи необходимо произвести вычисление коэффициентов ДПХ последовательности $g_x(t)$,

$$\hat{g}_{v_x} = \frac{1}{N}\sum_{t=0}^{K-1} g_x(t)\mathrm{cas}\left(\frac{2\pi v t}{K}\right). \qquad (3)$$

Величина коэффициента ДПХ зависит от положения на изображении движущегося объекта и сдвига v. Определение сдвига сводится к сравнению последовательности $g_x(t)$ с каждой последовательностью множества $\{\mathrm{cas}\left(\frac{2\pi v t}{K}\right)\}$ и выбору ближайшей из них по рассто-

янию Хэмминга. Максимальное значение коэффициента $\hat{g}_{v_x}$ определяет величину v. Это значение ДПХ формируется в точке с тем номером v функции $\hat{g}_{v_x}$, координата которой пропорциональна скорости движения объекта.

Аналогичные рассуждения справедливы для получения коэффициентов ДПХ в направлении оси y. Выражение проекции плоскости изображения кадра на ось y имеет вид

$$g_y(t) = \sum_{y=0}^{M-1}\sum_{x=0}^{N-1} g_{x,y,t}\,\mathrm{cas}\left(\frac{2\pi y}{M}\right), t = 0,1,\ldots,K-1. \quad (4)$$

1-ДПХ последовательность $g_y(t)$ определяется как

$$\hat{g}_{u_y} = \frac{1}{N}\sum_{t=0}^{K-1} g_y(t)\,\mathrm{cas}\left(\frac{2\pi u t}{K}\right). \quad (5)$$

Пусть наблюдаемый объект движется с равномерной скоростью. Сдвиг объекта по оси x за время между двумя кадрами равен p_x пикселов. За временной промежуток всего набора кадров сдвиг объекта составит $P_x = p_x K$ пикселов. Если известно расстояние d между пикселами, путь, пройденный объектом, равен $D = dP_x$. Время t_Σ, затраченное на съемку всех K кадров, можно найти, задавая частоту кадров f. Тогда получаем $t_\Sigma = \frac{K}{f}$. Зная расстояние D и время t_Σ, составляющая скорости движения объекта по оси x определяется соотношением

$$V_x = \frac{D}{t_\Sigma} = \frac{dP_x f}{K} = dp_x f\ . \quad (6)$$

Заменяя в (6) p_x на значение номера v коэффициента max $\hat{g}_{v_x}$, составляющая скорости

$$V_x = dvf. \quad (7)$$

Аналогично рассчитывается составляющая скорости по оси y:

$$V_y = duf. \quad (8)$$

Реальная физическая скорость объекта

$$V = \sqrt{V_x^2 + V_y^2}\ . \quad (9)$$

Таким образом, если известны: расстояние между пикселами d, частота съемки f и значения нормированных частот v и u становится возможным эффективное вычисление скорости движения, трудноразличимого глазом, объекта на изображении.

Оценка параметров движения объекта на основе ДПХ

Рассмотрим следующий пример. Пусть число кадров бинарного изображения $K = 16$. Объект наблюдения и фон изображения представляются единичными пикселами одинаковой яркости. Маскирование объекта достигается наложением на изображение шумовой маски. На рисунке показаны совмещенные изображения объекта интереса и шума в 2D пространстве. Иллюстрации отражают последовательное образование сцен временными и пространственными координатами. После 15 кадров съемки объект сдвинулся на 30 пикселов по оси x и на 15 пикселов по направлению оси y. Его положение определяется координатами (t_{15}, x_{30}, y_{15}) (рис. 1).

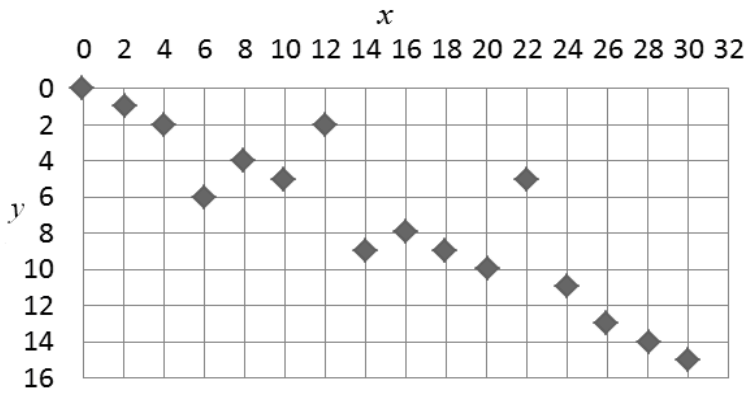


Рис. 1. Зашумленное пространственно-временное изображение сцен кадров

На рис. 2 и 3 представлены графики 1D спектров $\hat{g}_{v_x}$ и $\hat{g}_{u_y}$ преобразования Хартли последовательностей проекций $g_x(t)$ и $g_y(t)$, которые соответствуют изображению, показанному на рис. 1.

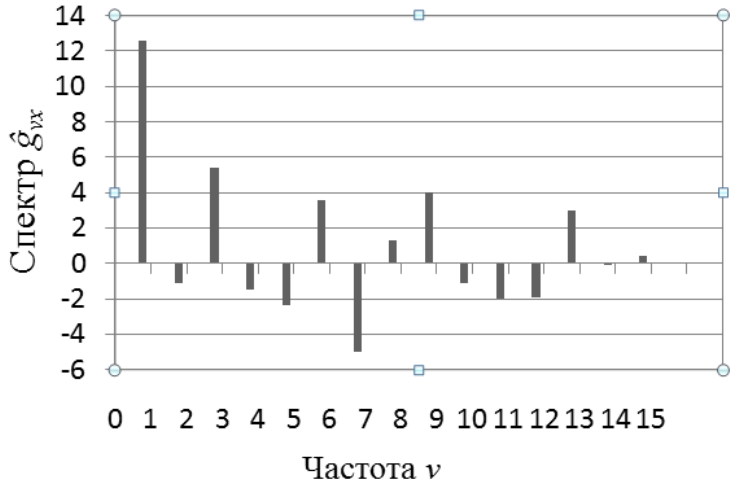


Рис. 2. Спектр последовательности $g_x(t)$

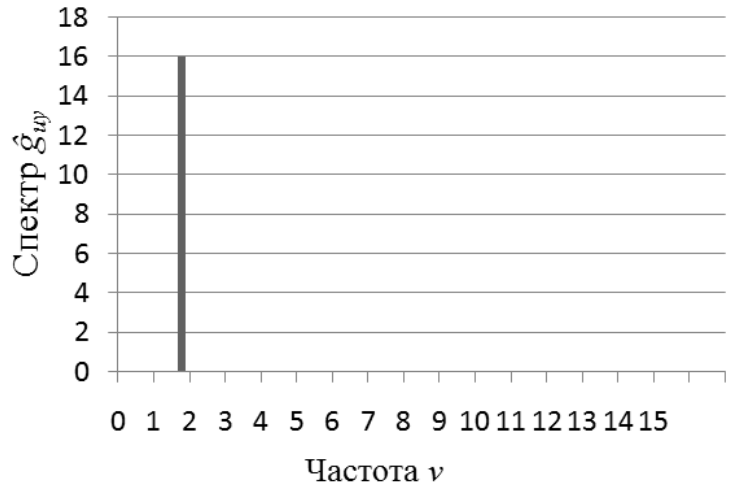


Рис. 3. Спектр последовательности $g_y(t)$

Как видно из графиков, движущийся объект характеризуется спектром, представленным в виде максимальных пиков. Искомые частотные параметры, необходимые для вычисления скорости движения объекта, равны соответственно $v=1$ и $u=2$. Спектральные составляющие других значений нормированных частот определяют уровень шума (маскирования). Ис-

пользуя формулы (7), (8) и (9), можно вычислить скорость движения объекта наблюдения. Пусть расстояние между пикселами $d = 2$ м, частота съемки $f = 32\frac{\text{кадр}}{\text{с}}$. Составляющие скоростей по оси x и оси y равны:

$$V_x = dvf = 2 \cdot 1 \cdot 32 = 64\frac{\text{м}}{\text{с}};\ V_y = duf = 2 \cdot 2 \cdot 32 = 128\frac{\text{м}}{\text{с}}.$$

Физическая скорость объекта составляет величину $V_x = 143{,}108\frac{\text{м}}{\text{с}}$.

Для обнаружения трудноразличимых движущихся объектов необходимо рассматривать изменения положения каждого пиксела на протяжении нескольких кадров. Увеличение времени наблюдения (числа кадров) уменьшает вероятность ошибочной оценки скорости. Неправильные значения координат наблюдаемого объекта, встречающиеся в последовательности кадров, в этом случае исправляются.

Заключение

Использование ДПХ в задачах, связанных с обработкой изображений, показывает его эффективность. В сравнении с комплексным алгоритмом ДПФ, применение ДПХ для анализа движения объектов дает сокращение количества выполняемых вычислительных операций. В ряде применений быстрый алгоритм ДПХ превосходит БПФ и может его заменять.

DETECTION OF CONCEALED MOVING OBJECTS

A.I. MITSIUKHIN

Abstract

The problem of detecting of hidden image of a moving object is considered. An estimation of the speed of given object, the direction of its movement and distance passed is required. The possibility of detection of dynamic images in frequency domain by using the discrete Hartley transform (DHT) is investigated.

Литература

1. *Mitsiukhin A.* // Innovation in Mechanical Engineering – Shaping the Future: Proceedings 56. International Scientific Colloquium, 12-16 September. 2011. P. 1-4.
2. *Gonzalez R.C., Woods R.E.* Digital Image Processing. NJ, 2002.

УДК 621.391

ОТНОСИТЕЛЬНАЯ ОЦЕНКА САМОПОДОБИЯ ТРАФИКА ВИДЕОКОНФЕРЕНЦ-СВЯЗИ НА ОСНОВЕ ПАРАМЕТРА ХЕРСТА

Ю.А. СЕЛИВАНОВА, У.М. АЛЬ-ХАСНАВИ, Л.Я. ВАРЕЦ

Белорусский государственный университет информатики и радиоэлектроники
П. Бровки, 6, Минск, 220013, Беларусь

Поступила в редакцию 14 марта 2012

Предложена методика относительной оценки самоподобия трафика видеоконференц-связи на основе параметра Херста. Сущность методики состоит в использовании разности между параметрами Херста, вычисленными с помощью одинаковых методов для видеопотоков в различных системах видеоконференц-связи при одинаковых условиях. Оценка самоподобия осуществляется по величине разности между параметрами Херста, которая должна быть положительной и может быть получена в результате усреднения по нескольким методам определения параметра Херста. Показано, что методика позволяет оценить эффективность систем видеоконференц-связи без использования специального измерительного оборудования.

Ключевые слова: параметр Херста, самоподобие, видеоконференц-связь.

Введение

Структура и параметры трафика оказывают существенное влияние на качество его обслуживания в сети. Наиболее остро проблема обеспечения качества обслуживания стоит для мультимедийного трафика, структура и параметры которого зависят от используемых методов кодирования. В связи с ростом популярности сервисов видеоконференц-связи данная проблема актуальна для локальных и глобальных сетей. Оценка необходимых сетевых ресурсов для обеспечения качества обслуживания видеотрафика часто производится на основе коэффициента использования канала [1], коэффициента пачечности трафика [2] и т.д. Эти методы достаточно просты, однако требуют специального измерительного оборудования и не учитывают самоподобную структуру видеотрафика и, как следствие, дают неверную оценку. На оценку самоподобия ориентированы методы анализа трафика, основанные на вычислении параметра Херста [3], однако они часто дают противоречивые результаты. Возможным решением проблемы является использование относительных оценок самоподобия.

Целью работы является разработка методики относительной оценки самоподобия трафика видеоконференц-связи на основе параметра Херста.

Параметр Херста и методы его оценки

Для оценки самоподобных свойств трафика часто используется коэффициент Херста – H. Если данный коэффициент находится в пределах $0{,}5<H<1$, то исследуемый процесс проявляет самоподобные свойства. Приближение H к 1 говорит о высокой самоподобности процесса и о том, что поведение процесса является персистентным или процесс обладает длительной памятью. Т.е., если на некотором временном промежутке наблюдалось приращение показателей процесса, то и в будущем в среднем будет происходить увеличение.

При $H=0{,}5$ отклонение процесса от среднего является случайными и не зависит от предыдущих значений.

При 0<*H*<0,5 процесс является переменчивым, т.е. увеличение относительно среднего в прошлом, в будущем сменится в противоположном направлении.

Для анализа самоподобного мультимедийного трафика применяется несколько методов. Метод анализа изменения дисперсии [4] основан на том, что для агрегированных временных серий $X(k)^{(m)}$ самоподобного процесса дисперсия при больших значениях *m* подчиняется формуле $Var[X(k)^{(m)}] \sim \frac{Var[X(t)]}{m^{\beta}}$. Здесь параметр самоподобия $H = 1-(\beta/2)$. В результате логарифмирования этой формулы получается:

$$\log[Var[X(k)^{(m)}]] \sim \log[Var[X(t)]] - \beta\log(m). \quad (1)$$

Т.к. $\log[Var[X(t)]]$ не зависит от *m*, то график зависимости $Var[X(k)^{(m)}]$ от *m* в логарифмическом масштабе представляет прямую линию с наклоном, равным минус β. График можно построить по набору данных $X(t)$, если сгенерировать агрегированный процесс на разных уровнях агрегации *m*, а затем вычислить дисперсию. После этого по графику находится значение параметра *H*. Тангенс угла наклона от минус одного до нуля предполагает наличие самоподобия.

При анализе нормированного размаха [5] для стохастического процесса $X(t)$, определенного в дискретные моменты времени $\{X_t, t = 0, 1, 2, ...\}$, диапазон $X(t)$ в измененном масштабе шкалы за интервал времени *N* определяется как отношение

$$\frac{R}{S} = \frac{\max\limits_{1 \le j \le N}\left[\sum\limits_{k=1}^{j}(X_k - M(N))\right] - \min\limits_{1 \le j \le N}\left[\sum\limits_{k=1}^{j}(X_k - M(N))\right]}{\sqrt{\frac{1}{N}\cdot\sum\limits_{k=1}^{N}(X_k - M(N))^2}}, \quad (2)$$

где $M(N)$ – выборочное среднее за период времени *N*, определяемое с помощью выражения

$$M(N) = \frac{1}{N}\cdot\sum_{j=1}^{N} X_j. \quad (3)$$

В числителе формулы (2) находится величина интервала процесса, а в знаменателе – выборочное среднеквадратичное. Для самоподобного процесса это отношение при больших значениях *N* обладает следующей характеристикой:

$$R/S \sim (N/2)^H. \quad (4)$$

В результате логарифмирования обеих частей выражения (4) получается:

$$\log[R/S] \sim H\cdot\log(N) - H\cdot\log(2). \quad (5)$$

Если построить график зависимости $\log[R/S]$ от *N* в логарифмическом масштабе, то получается прямая линия с наклоном, равным *H*.

Оценка, основанная на графике спектральной плотности, составляет суть периодограммного метода, который обеспечивает большую статистическую строгость, чем рассмотренные выше оценки [6]. Однако для использования данного метода необходимо, чтобы параметризованная модель процесса была известна. Периодограмма (функция интенсивности) $I_N(\omega)$ представляет собой спектральную плотность дискретного стохастического процесса $X(t)$ и может быть оценена следующим рядом на интервале времени *N* при $\omega \in [0, \pi]$:

$$I_N(\omega) = \frac{1}{2\cdot\pi\cdot N}\cdot\left|\sum_{k=1}^{N} X_k \cdot e^{jk\cdot\omega}\right|^2. \quad (6)$$

При $\omega \to 0$ формируется зависимость спектральной плотности вида:

$$I_N(\omega) \sim \omega^{1-2\cdot H}. \quad (7)$$

Для зависимости $\log[I_N(\omega)]$ от $\log(\omega)$ (только для нижних частот), подбирается касательная прямая линия к кривой. Наклон линии приблизительно равен $1-2\cdot H$.

Методика относительной оценки самоподобия трафика видеоконференц-связи на основе параметра Херста

Предлагается методика относительной оценки самоподобия трафика видеоконференц-связи на основе параметра Херста. Сущность методики состоит в использовании разности между параметрами Херста, вычисленными с помощью одинаковых методов для видеопотоков в различных системах видеоконференц-связи при одинаковых условиях. Оценка самоподобия осуществляется по величине разности между параметрами Херста, которая должна быть положительной и может быть получена в результате усреднения по нескольким методам определения параметра Херста. На рисунке приведена схема измерения характеристик трафика для вычисления параметра Херста.

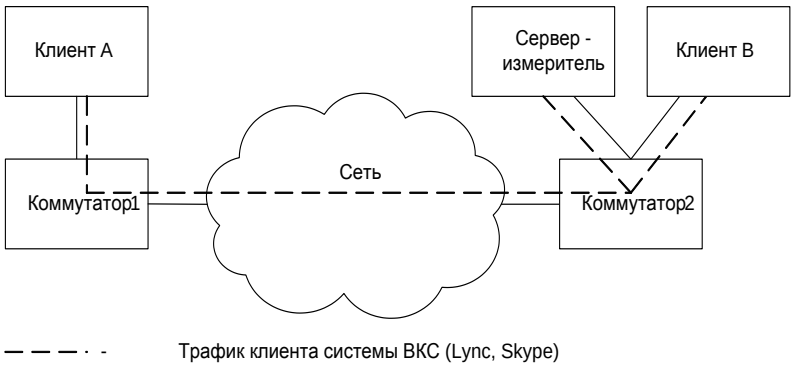


Схема измерения характеристик трафика для вычисления параметра Херста

К порту коммутатора 2 (Cisco 1900) по интерфейсу RJ-45 (10 Мбит/с) подключен компьютер с измерительным ПО Wireshark. Выбранный порт устройства сконфигурирован в режиме SPAN для зеркального отображения данных, поступающих в коммутатор, т.е. симплексный Rx-канал. Измерительное ПО выполняет измерение задержек поступающих пакетов с точностью до 1 мкс.

Результаты экспериментов по относительной оценке самоподобия

Для сравнения выбраны две системы видеоконференц-связи: Microsoft Lync 2010 и Skype. Для каждой из систем протестировано три режима работы в течении 60 сек: трансляция видео без звука, трансляция видео со звуком и трансляция рабочего стола компьютера. В результате захвата пакетов получены шесть реализаций сетевого трафика: Dump-1 – Dump-6. Реализация Dump-1 получена при трансляции видео с низкой динамикой (low motion) и Dump-2 – при трансляции видео с высокой динамикой (high motion) в режиме без звука; Dump-3 – при трансляции видео (low motion) и Dump-4 – при трансляции видео (high motion) одновременно с аудио; Dump-5 – при трансляции презентации (low motion) и Dump-6 – при трансляции презентации (high motion).

В данной работе для исследования структуры трафика видеоконференцсвязи и иллюстрации его фрактального (самоподобного) характера использовались три метода оценки коэффициента Херста: анализ изменения дисперсии (AggrVar), анализ нормированного размаха (R/S) и периодограммный анализ (Period), реализованные в математическом пакете Matlab. Использование разнообразных методов оценки показателя Херста преследовало цель получить более достоверные результаты.

Результаты оценки различными методами представлены в таблице. Значение показателя Херста для всех рассмотренных реализаций близко к 0,5, что свойственно для белого шума. Усредненное значение H для сетевого трафика системы Lync больше (H~0,5252), чем для системы Skype (H~0,4349). Это свидетельствует о более эффективном кодировании видеоданных в Lync.

Результаты оценки показателя самоподобия

System	Lync				Skype			
Method	AggrVar	R/S	Period	Avg	AggrVar	R/S	Period	Avg
Dump-1	0,5968	0,5507	0,6213	0,5896	0,1163	0,2629	0,4791	0,2861
Dump-2	0,4293	0,4774	0,4119	0,4395	0,4983	0,4458	0,4835	0,4759
Dump-3	0,5212	0,5681	0,5770	0,5554	0,4369	0,4397	0,4132	0,4299
Dump-4	0,5787	0,5023	0,5483	0,5431	0,5223	0,5215	0,4738	0,5059
Dump-5	0,5382	0,5739	0,4717	0,5279	0,4765	0,4421	0,4683	0,4623
Dump-6	0,6019	0,5458	0,5393	0,5623	0,4139	0,4399	0,3430	0,3989
Среднее значение по Dump-1 – Dump-6				0,5252	Среднее значение по Dump-1 – Dump-6			0,4349

Заключение

Предложена методика относительной оценки самоподобия трафика видеоконференц-связи на основе параметра Херста. Сущность методики состоит в использовании разности между параметрами Херста, вычисленными с помощью одинаковых методов для видеопотоков в различных системах видеоконференц-связи при одинаковых условиях. Оценка самоподобия осуществляется по величине разности между параметрами Херста, которая должна быть положительной и может быть получена в результате усреднения по нескольким методам определения параметра Херста.

COMPARATIVE EVALUATION OF SELF-SIMILARITY OF A VIDEOCONFERENCING TRAFFIC BASED ON HURST PARAMETER

Y.A. SELIVANAVA, O.M. AL-HASNAWI, L.Y. VARETS

Abstract

The technique for a relative assessment of self-similarity of a video conferencing traffic based on Hurst's parameter is offered. The entity of this technique consists in use differences between Hurst's parameters calculated by means of identical methods for videostreams in various systems of a videoconferencing under identical conditions. The estimation of self-similarity is carried out on difference in size between Hurst's parameters which should be positive and can be obtained by averaging over a number of methods of determining the Hurst parameter. It is shown that the technique allows to estimate the efficiency of videoconferencing systems without the use of special measuring equipment.

Литература

1. *Васькин Ю.А.* // T-Comm. Телекоммуникации и транспорт. Технологии информационного общества. 2009. С. 4-7.
2. *Шувалов В.П.* Телекоммуникационные системы и сети. Том 3. Мультисервисные сети М., 2005.
3. *Leland W.E.* // IEEE/ACM Transactions on Networking. 1994. Vol. 2, №1. P. 1-15.
4. *Park K.* // Self-Similar Network Traffic: An Overview. 2003. P.19-22.
5. *Beran J.* Statistics For Long-Memory Processes. 1994.
6. *Taqqu M.* // A practical guide to heavy tails. 1996. P. 177-217.

УДК 612.391

АЛГОРИТМ ВЫЧИСЛЕНИЯ БИНАРНОГО ДИСКРЕТНОГО ВЕЙВЛЕТ-ПРЕОБРАЗОВАНИЯ НА ОСНОВЕ ЛИФТИНГ-СХЕМЫ

Л.А. РУИС, А.А. БОРИСКЕВИЧ

Белорусский государственный университет информатики и радиоэлектроники
П. Бровки, 6, Минск, 220013, Беларусь

Поступила в редакцию 11 октября 2012

Предложен алгоритм вычисления бинарного дискретного вейвлет-преобразования на основе лифтинг-схемы, обеспечивающего низкую вычислительную сложность, низкий объем бинарных промежуточных данных, отсутствие эффектов и ошибок квантования, а также отсутствие изменения исходного динамического диапазона изображений в вейвлет-области. Алгоритм обеспечивает увеличение концентрации энергии в минимальном количестве вейвлет-коэффициентов изображения по критерию оценки спектра собственных значений преобразованной корреляционной матрицы последовательности Маркова первого порядка.

Ключевые слова: бинарное вейвлет-преобразование, спектр собственных значений, лифтинг-схема.

Введение

В современных системах предварительной обработки и постобработки, сжатия, анализа и защиты изображений широко используется дискретное вейвлет-преобразование (ДВП), обладающее низкой вычислительной сложностью, свойством компактности энергии, возможностью выбора базисных вейвлет-функций с различной пространственно-частотной локализацией, гладкостью и симметрией.

Стандартная реализация ДВП основана на банке КИХ-фильтров, что требует большого количества вычислительных операций и существенно увеличивает используемый объем памяти. В последнее время предложено новое математическое определение вейвлет-преобразования, основанное на пространственно-частотных свойствах вейвлет-функций и гибкой схеме факторизации банка фильтров. Данный подход получил название лифтинг-схемы (ЛС) или лифтинг вейвлет-преобразования (ЛВП) [1]. Вейвлет-преобразование применяется для многих приложений, включая обнаружение края [2], [3], сжатие и кодирования изображений [4], [5], фильтрации сигналов [6], [7], стохастические процессы, фрактальные модели [8-10], частотно-временной анализ [11], [12], радар [13], [14] и др.

Препятствием для улучшения характеристик эффективности лифтинг-схем является использование традиционным ДВП небинарных банков фильтров.

В связи с этим целью работы является разработка алгоритма вычисления бинарного дискретного вейвлет-преобразования на основе лифтинг-схемы, обеспечивающего низкую вычислительную сложность, низкий объем бинарных промежуточных данных, отсутствие эффектов и ошибок квантования, а также отсутствие изменения исходного динамического диапазона изображений в вейвлет-области.

Бинарное дискретное вейвлет-преобразования

Поле – это любая арифметическая система, в которой можно складывать, вычитать, умножать и делить в соответствии с обычными свойствами ассоциативности, дистрибутивности и коммутативности. Конечное поле (Галуа) обозначается $GF(p)$, где p – порядок поля.

Если p является простым числом, то $GF(p)$ можно представить в виде множества элементов $\{0,1,2,...,p-1\}$ с операциями сложения и умножения по модулю p. Допустим, что вейвлет-декомпозицией является конечное поле с учетом параметров обрабатываемого сигнала (например, изображения). Тогда возможно осуществить бинарное дискретное вейвлет-преобразование (БДВП), в котором арифметика выполняется полностью в $GF(2)$, т.е. в поле с бинарными элементами $\{0,1\}$ и арифметическими операциями по модулю-2.

БДВП имеет те же свойства, что и традиционное дискретное вейвлет-преобразование (дискретное лифтинг ВП – ДЛВП), но, кроме того, обладает следующими преимуществами:

- низкая вычислительная сложность, так как используется арифметика по модулю-2 и операции сдвига;
- промежуточные и конечные данные являются бинарными;
- не вносит никаких эффектов и ошибок квантования, что всегда гарантирует полную обратимость;
- не изменяет в вейвлет-области исходный динамический диапазон изображений.

Для обеспечения обратимости вейвлет-преобразований с требуемыми многомасштабными свойствами процесс реализации схемы банка фильтров БДВП должен основываться на учете трех основных ограничений на параметрах бинарных фильтров [15]: ширине полосы пропускания, совершенном восстановлении и количестве нулевых моментов.

Аналогично традиционному ДВП на основе банка фильтров БДВП осуществляется бинарными фильтрами посредством круговой бинарной свертки и операции прореживания. Матрица прямого преобразования (TM) БДВП имеет следующий вид:

$$
\begin{aligned}
&TM = \begin{bmatrix} H \\ G \end{bmatrix}_{NxN}, \\
&H = \left[\bar{C}\big|_{s=0}, \bar{C}\big|_{s=2}, ..., \bar{C}\big|_{s=N-2} \right]^T, \\
&G = \left[\bar{D}\big|_{s=0}, \bar{D}\big|_{s=2}, ..., \bar{D}\big|_{s=N-2} \right]^T, \\
&\bar{C} = \{c_0, c_1, ..., c_{N-2}, c_{N-1}\}, \\
&\bar{D} = \{d_0, d_1, ..., d_{N-2}, d_{N-1}\},
\end{aligned}
\qquad (1)
$$

где $\bar{A}\big|_{s=k}$ – вектор с элементами, сформированными с помощью операции их кругового k-го сдвига вправо при условии, что $k = 2n$ и $n = \overline{0, \frac{N}{2}-1}$; G и H – подматрицы для преобразования бинарного поля фильтра (ПБПФ) [15]; T – символ транспонирования; $\bar{C}$ и $\bar{D}$ – аппроксимационный и детализирующий бинарные фильтры с весовыми коэффициентами c_i и d_i без учета сдвига, соответственно; $i = \overline{0, N-1}$.

Таким образом, БДВП на основе банка фильтров осуществляется умножением матрицы TM на последовательность входных данных x, что приводит к их одновременной фильтрации и прореживанию:

$$y = TM\, x, \qquad (2)$$

где x – исходный сигнал и y – вейвлет-спектр.

Ограничение ширины полосы пропускания удовлетворяется, если обеспечивается приблизительно равное количество ненулевых столбцов в подматрицах ПБПФ, и одинаковые длины $\bar{D}$ и $\bar{C}$ фильтров. В случае соблюдения данных ограничений последний столбец подматрицы G для высокочастотного фильтра $\bar{D}$ имеет вид

$$G(\overline{0, N-1}; N-1) = \begin{bmatrix} 0 \\ \vdots \\ 0 \end{bmatrix}. \qquad (3)$$

Выполнение данного ограничения поддерживает равномерным распределение контента выходной последовательности высоко- и низкочастотного фильтров, что позволяет проводить многомасштабное разложение входных данных без потери информации при их прореживании.

Для обеспечения относительной степени гладкости в пространственной вейвлет-области с целью компактного представления медленно меняющихся данных сигнала необходимо, чтобы вейвлет-фильтр имел соответствующее количество нулевых моментов N_{vm}, которое пропорционально количеству последовательных нулей в подматрицах ПБПФ. Оно задается коэффициентом кругового сдвига k: $N_{vm} \approx k$.

Реализация совершенного восстановления схемой банка фильтров требует наличия свойства обратимости у матрицы преобразования TM размером $N \times N$. Оно обеспечивается тогда и только тогда, когда ее детерминант равен единице $\det(TM) = 1$ с учетом того, что единственный ненулевой элемент в $GF(2)$ равен единице [16].

Для упрощения вычисления детерминанта матрицу преобразования можно представить в форме верхней матрицы Хессенберга (ВМХ) [15], которая характеризуется тем, что ее подматрицы размером $N/2 \times N/2$, находящие вдоль главной диагонали, являются одинаковыми:

$$TM = \begin{bmatrix} \sum_{i=2n}^{N-2} c_i & \sum_{i=2n+1}^{N-1} c_i \\ \sum_{i=2n}^{N-2} d_i & \sum_{i=2n+1}^{N-1} d_i \end{bmatrix}. \qquad (4)$$

В этом случае детерминант ВМХ определяется с помощью соотношения

$$\det(TM) = \sum_{i=2n}^{N-2} c_i \sum_{i=2n+1}^{N-1} d_i + \sum_{i=2n+1}^{N-1} c_i \sum_{i=2n}^{N-2} d_i = 1$$

при $\sum_{i=2n}^{N-2} c_i = 0$, $\sum_{i=2n+1}^{N-1} c_i = 1$, $\sum_{i=2n}^{N-2} d_i = 1$, $\sum_{i=2n+1}^{N-1} d_i = 1$.

Для гарантии обратимости БДВП требуется, чтобы выполнялось равенство

$$d_{2i+1} = d_{2i} \qquad (5)$$

при $0 \le n < N/2$.

Возможность использования данного подхода обусловлена тем фактом, что $a^p = a$ для любого $a \in GF(2)$ при целом числе $p \ge 1$, т.е. умножение $N/2$-х одинаковых элементов равно исходному элементу в $GF(2)$.

Обратное БДВП имеет вид

$$x = UM\, y. \qquad (6)$$

Аналогично матрице прямого преобразования, матрица обратного преобразования UM определяется выражением

$$\begin{aligned} &UM = [S\ R]_{NxN}, \\ &S = \left[\bar{S}\big|_{s=0}, \bar{S}\big|_{s=2}, ..., \bar{S}\big|_{s=N-2} \right], \\ &R = \left[\bar{R}\big|_{s=0}, \bar{R}\big|_{s=2}, ..., \bar{R}\big|_{s=N-2} \right], \\ &\bar{R} = \{r_0, r_1, ..., r_{N-2}, r_{N-1}\}^T, \\ &\bar{S} = \{s_0, s_1, ..., s_{N-2}, s_{N-1}\}^T, \end{aligned} \qquad (7)$$

где R и S – подматрицы для обратных ПБПФ; $\bar{R}$ и $\bar{S}$ – аппроксимационные и детализирующие обратные фильтры без учета сдвига с весовыми коэффициентами r_i и s_i соответственно; $i=\overline{0,N-1}$.

Условия независимости БДВП от длительности сигнала

Рассмотренные ограничения гарантируют обратимость БДВП, но не обеспечивают свойство ортогональности и биортогональности БДВП. Это обусловлено тем, что изменения длины сигнала, как и в процессе увеличения разрешения (восстановления), приводят к изменению длины обратных бинарных фильтров. Согласно (5), энергия высоко- E_D и низкочастотного E_C фильтров подчиняется соотношениям

$$E_C=\sum_{i=0}^{N-1}c_i=1 \text{ и } E_D=\sum_{i=0}^{N-1}d_i=0. \tag{8}$$

В отличие от традиционного ДВП вектор, принадлежащий $GF(2)$, может иметь нулевую энергию даже тогда, когда вектор не является нулевым вектором. Поскольку энергия высокочастотного фильтра равна нулю, то БДВП не может быть ортогональным или биортогональным, хотя оно обратимо. Отсутствие ортогональности и биортогональности требует усложнения реализации обратных бинарных фильтров.

Для того, чтобы обратные бинарные фильтры не зависели от длительности сигнала, используется дополнительное ограничение перпендикулярности [17], которое определяется посредством следующих условий:

$$\bar{C}\cdot\bar{R}\big|_{s=j}=\delta_j,\ \bar{C}\cdot\bar{S}\big|_{s=j}=0,\ \bar{D}\cdot\bar{R}\big|_{s=j}=0,\ \bar{D}\cdot\bar{S}\big|_{s=j}=\delta_j \tag{9}$$

где $\delta_j=\begin{cases}1 & \text{при } j=0\\ 0 & \text{иначе}\end{cases}$; $A\cdot B$ – векторное скалярное произведение векторов A и B; $j=2n$ при $n=\overline{0,\frac{N}{2}-1}$. Данное условие (9) должно выполняться для всех сигналов, имеющих длину больше или равной длине фильтров. Если выполняются условия (5), (8) и (9), то система уравнений для определения r и c при длине прямых бинарных фильтров $N=8$ имеет вид

$$\begin{bmatrix} c_0 & c_1 & c_2 & c_3 & c_4 & c_5 & c_6 & c_7\\ 0 & 0 & c_0 & c_1 & c_2 & c_3 & c_4 & c_5\\ 0 & 0 & 0 & 0 & c_0 & c_1 & c_2 & c_3\\ 0 & 0 & 0 & 0 & 0 & 0 & c_0 & c_1\\ c_6 & c_7 & 0 & 0 & 0 & 0 & 0 & 0\\ c_4 & c_5 & c_6 & c_7 & 0 & 0 & 0 & 0\\ c_2 & c_3 & c_4 & c_5 & c_6 & c_7 & 0 & 0\\ d_0 & d_1 & d_2 & d_3 & d_4 & d_5 & d_6 & d_7\\ 0 & 0 & d_0 & d_1 & d_2 & d_3 & d_4 & d_5\\ 0 & 0 & 0 & 0 & d_0 & d_1 & d_2 & d_3\\ 0 & 0 & 0 & 0 & 0 & 0 & d_0 & d_1\\ d_6 & d_7 & 0 & 0 & 0 & 0 & 0 & 0\\ d_4 & d_5 & d_6 & d_7 & 0 & 0 & 0 & 0\\ d_2 & d_3 & d_4 & d_5 & d_6 & d_7 & 0 & 0 \end{bmatrix} \begin{bmatrix} r_0 & s_0\\ r_1 & s_1\\ r_2 & s_2\\ r_3 & s_3\\ r_4 & s_4\\ r_5 & s_5\\ r_6 & s_6\\ r_7 & s_7 \end{bmatrix} = \begin{bmatrix} 1 & 0\\ 0 & 0\\ 0 & 0\\ 0 & 0\\ 0 & 0\\ 0 & 0\\ 0 & 0\\ 0 & 1\\ 0 & 0\\ 0 & 0\\ 0 & 0\\ 0 & 0\\ 0 & 0\\ 0 & 0 \end{bmatrix} \tag{10}$$

Из (10) видно, что решение данной системы уравнений зависит от весовых коэффициентов выбранных прямых бинарных фильтров d и c, что приводит к четырем группам пар бинарных фильтров, которые согласованы с ограничениями вычисления БДВП (см. табл. 1).

Таблица 1. **Группы пар бинарных фильтров длиной $N=8$**

Группа	Тип фильтра	Выбранные прямые бинарные фильтры	Колич. возможных реализаций обратных фильтров
1	НЧ ВЧ	$\{0,1,0,0,0,0,0,0\}$ $\{1,1,0,0,0,0,0,0\}$	4
2	НЧ ВЧ	$\{1,1,1,0,0,0,0,0\}$ $\{1,1,0,0,0,0,0,0\}$	12
3	НЧ ВЧ	$\{1,1,1,1,0,0,0,1\}$ $\{1,1,0,0,0,0,0,0\}$	12
4	НЧ ВЧ	$\{1,1,1,1,1,1,1,0\}$ $\{1,1,0,0,0,0,0,0\}$	4

Лифтинг-схема бинарного ДВП

БДВП, как и традиционное ДВП, на основе банка фильтров имеет ряд недостатков: высокая вычислительная сложность и большой объем промежуточных коэффициентов при процессе фильтрации и прореживании. Для устранения данных недостатков была предложена лифтинг-схема для дискретного вейвлет-преобразования [1]. Переход от БДВП на основе банка фильтров к лифтинг-схеме БДВП основан на подходе, представленном в [18].

Аппроксимационный фильтр $\bar{C}$ можно представить в виде полиномов Лаурента в Z-области следующим образом:

$$\bar{C}(z)=\sum_{q=k_b}^{k_e} c_q z^q ,$$

где k_b и k_e – наименьшее и наибольшее целые числа, соответственно, при которых $c_q \in GF(2)$ является ненулем, а степень полинома определяется $\deg\left|\bar{C}\right| = k_e - k_b$, причем $\deg\left|\bar{C}\right| = 0$ когда $\bar{C}$ является мономом.

В полифазном представлении фильтр $\bar{C}$ можно представить в виде

$$\bar{C}(z)=c_e\left(z^2\right)+z^{-1}c_o\left(z^2\right), \qquad (11)$$

где c_e и c_o – четные и нечетные отсчеты импульсной характеристики фильтра, соответственно.

Аналогично в полифазном виде можно представить и остальные фильтры и исходный сигнал:

$$\bar{D}(z)=d_e\left(z^2\right)+z^{-1}d_o\left(z^2\right),$$

$$\bar{R}(z)=r_e\left(z^2\right)+z^{-1}r_o\left(z^2\right), \qquad (12)$$

$$\bar{S}(z)=s_e\left(z^2\right)+z^{-1}s_o\left(z^2\right),$$

$$X(z)=X_e\left(z^2\right)+z^{-1}X_o\left(z^2\right),$$

где X_e и X_o – четные и нечетные отсчеты исходного сигнала соответственно.

С учетом (11) и (12) определяются прямая PM и обратная BM полифазные матрицы:

$$PM(z)=\begin{bmatrix} c_e(z) & c_o(z) \\ d_e(z) & d_o(z) \end{bmatrix} \text{ и } BM(z)=\begin{bmatrix} r_e(z) & r_o(z) \\ s_e(z) & s_o(z) \end{bmatrix}. \qquad (13)$$

Следовательно, БДВП можно представить в виде произведения полифазных матриц:

$$\begin{bmatrix} Y_e(z) \\ Y_o(z) \end{bmatrix} = PM(z^{-1}) \begin{bmatrix} X_e(z) \\ X_o(z) \end{bmatrix} = \begin{bmatrix} c_e(z) & z^{-1}c_o(z) \\ d_e(z) & z^{-1}d_o(z) \end{bmatrix} \begin{bmatrix} X_e(z) \\ X_o(z) \end{bmatrix},$$
$$\begin{bmatrix} X_e(z) \\ X_o(z) \end{bmatrix} = BM(z) \begin{bmatrix} Y_e(z) \\ Y_o(z) \end{bmatrix} = \begin{bmatrix} r_e(z) & r_o(z) \\ s_e(z) & s_o(z) \end{bmatrix} \begin{bmatrix} Y_e(z) \\ Y_o(z) \end{bmatrix}. \quad (14)$$

В матричной форме (13) условие совершенного восстановления будет выглядеть следующим образом:

$$PM(z^{-1})BM(z) = I_{2\times 2},$$

где I – единичная матрица размером 2×2.

Если детерминант PM не является мономом, т.е. $\det(PM) \neq z^l$ при некоторых l целых числах, то его обратная величина приведет к неопределенности решений. Таким образом, предполагается, что детерминант PM всегда может быть определен в виде $\det(PM) = z^l$.

Не нарушая общности, можно считать, что детерминант $\det(PM) = z^l = 1$. В противном случае полиномы всегда можно разделить на их детерминанты, что эквивалентно сдвигу коэффициентов соответствующих бинарных фильтров в пространственной области. В связи с этим, пара фильтров синтеза $(\bar{C}, \bar{D})$ и пара фильтров анализа $(\bar{R}, \bar{S})$ являются комплементарными, и полифазные матрицы могут быть изменены следующим образом

$$PP(z) = \begin{bmatrix} m_e(z) & m_o(z) \\ n_e(z) & n_o(z) \end{bmatrix}.$$

Согласно (14) и с учетом зависимости между степенями полиномов $m_e(z)$, $m_o(z)$, $n_e(z)$ и $n_o(z)$, можно определить две различные структуры факторизации $PP(z)$ с помощью алгоритма Евклида на основе произведения конечного числа треугольных матриц.

Факторизация №1. Если $\deg|m_e(z)| \geq \deg|n_e(z)| \geq 0$ и $\deg|m_o(z)| \geq \deg|n_o(z)| \geq 0$, то существуют полиномы Лаурента $f_1(z)$, $m_e^{new}(z)$ и $m_o^{new}(z)$, которые удовлетворяют следующим уравнениям:

$$0 \leq \deg|m_e^{new}(z)| \leq \deg|n_e(z)|,$$

$$0 \leq \deg|m_o^{new}(z)| \leq \deg|n_o(z)|,$$

$$m_e(z) = m_e^{new}(z) + f_1(z)n_e(z),$$

$$m_o(z) = m_o^{new}(z) + f_1(z)n_o(z).$$

Это обуславливает снижение степеней $m_e(z)$ и $m_o(z)$ так, что они становятся меньше или равны $n_e(z)$ и $n_o(z)$ соответственно. В этом случает полифазную матрицу можно представить в виде

$$\begin{bmatrix} m_e(z) & m_o(z) \\ n_e(z) & n_o(z) \end{bmatrix} = \begin{bmatrix} 1 & f_1(z) \\ 0 & 1 \end{bmatrix} \begin{bmatrix} m_e^{new}(z) & m_0^{new}(z) \\ n_e(z) & n_o(z) \end{bmatrix}. \quad (15)$$

Факторизация №2. Если $\deg|n_e(z)| \geq \deg|m_e(z)| \geq 0$ и $\deg|n_o(z)| \geq \deg|m_o(z)| \geq 0$, то существуют полиномы Лаурента $t_1(z)$, $m_e^{new}(z)$ и $m_o^{new}(z)$, которые удовлетворяют следующим уравнениям:

$$0 \le \deg\left|n_e^{new}(z)\right| \le \deg\left|m_e(z)\right|,$$

$$0 \le \deg\left|n_o^{new}(z)\right| \le \deg\left|m_o(z)\right|,$$

$$n_e(z) = n_e^{new}(z) + t_1(z)m_e(z),$$

$$n_o(z) = n_o^{new}(z) + t_1(z)m_o(z).$$

Это аналогично обуславливает снижение степеней $n_e(z)$ и $n_o(z)$ так, что они становятся меньше или равны $m_e(z)$ и $m_o(z)$, соответственно. В этом случает полифазную матрицу можно представить в виде

$$\begin{bmatrix} m_e(z) & m_o(z) \\ n_e(z) & n_o(z) \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ t_1(z) & 1 \end{bmatrix} \begin{bmatrix} m_e(z) & m_o(z) \\ n_e^{new}(z) & n_0^{new}(z) \end{bmatrix}. \quad (16)$$

Комбинируя выражения (15) и (16), полифазная матрица всегда может быть разложена в виде произведения треугольных матриц двух типов следующим образом

$$PP(z) = \begin{bmatrix} m_e(z) & m_o(z) \\ n_e(z) & n_o(z) \end{bmatrix} = \prod_{i=1}^{n} \begin{bmatrix} 1 & f_i(z) \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ t_i(z) & 1 \end{bmatrix}. \quad (17)$$

Отметим, что факторизация в (17) отличается от лифтинг-схемы в традиционном ДВП. Это связано с тем, что имеется только два элемента в бинарном поле $GF(2)$. В результате, есть только один способ факторизации элемента 1, т.е. $1 = 1 \times 1$, в отличие от случая реального поля, где имеются бесконечные способы факторизации, т.е. $1 = K \times K^{-1}$.

Бинарное дискретное лифтинг вейвлет-преобразование БДЛВП применяется на бинарных изображениях, поэтому для его применения на полутоновых изображениях необходима предварительная декомпозиция на 8 битовых плоскостей (см. рис. 2). БДЛВП сначала осуществляется на каждом бинарном изображении, а потом объединяются все вейвлет-матрицы битовых плоскостей (рис. 1).

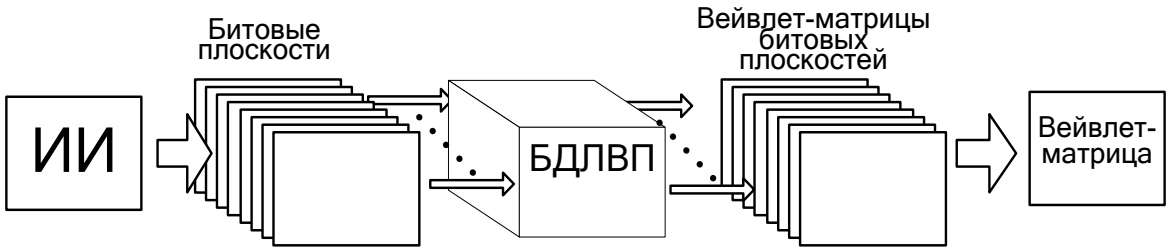
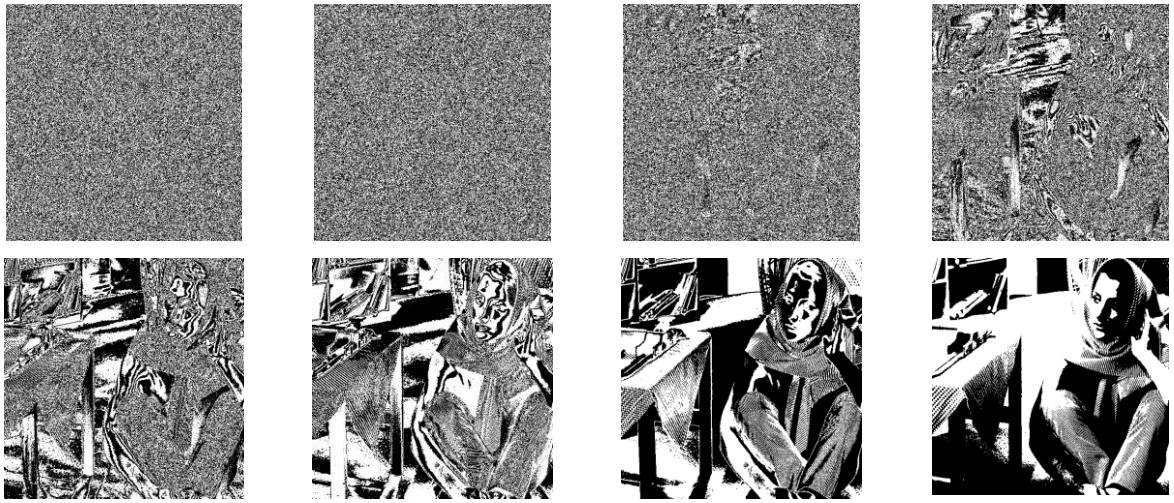
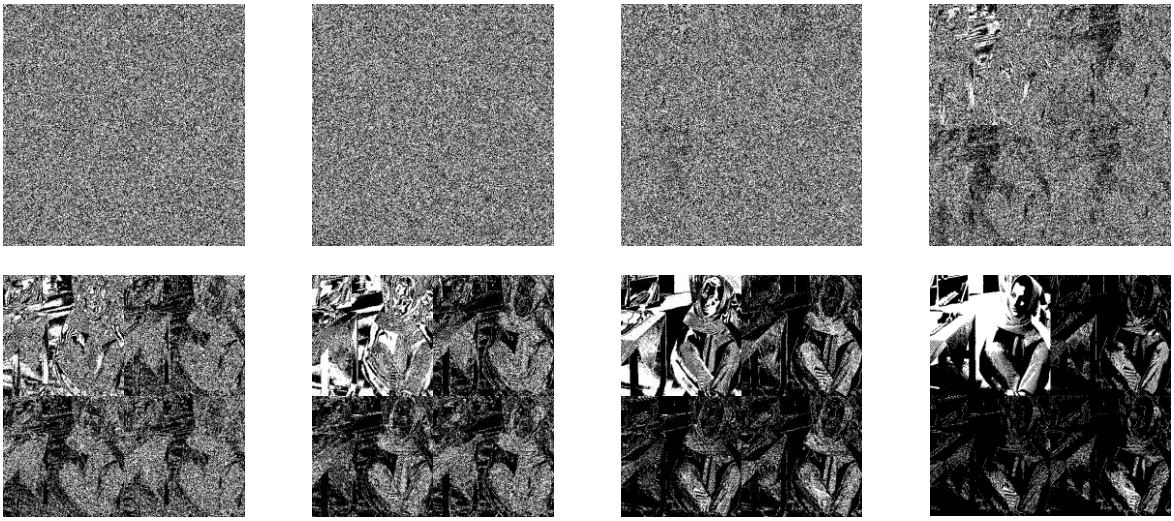


Рис. 1. Блок-схема БДЛВП



а



б

Рис. 2. Декомпозиция исходного изображения на 8 битовых плоскостей в простронтвенной (*а*) и вейвлет области (*б*)

Результаты моделирования

Для оценки эффективности предложенного алгоритма использованы вейвлет-функции Haar, 5/3, 7/5, 9/7 без адаптации и АЛВПК [19], АЛВПГ (алгоритм вычисления адаптивного обобщенного лифтинг вейвлет-преобразования без дополнительной информации) с адаптацией, и корреляционная матрица размером 16×16 последовательности Маркова первого порядка с коэффициентом корреляции $\rho = 0,95$.

Любой случайный дискретный сигнал $x(n)$ можно представить в виде последовательности Маркова p-го порядка, если условная вероятность текущего отчета $P\left(x\left(n\right)\right)$ удовлетворяет следующему соотношению [20], т.е.

$$P\left(x(n)\middle| x(n-1), x(n-2),...\right) = P\left(x(n)\middle| x(n-1), x(n-2),..., x(n-p)\right).$$

Корреляционная матрица R последовательности Маркова первого порядка с коэффициентом корреляции ρ [20] имеет вид

$$R = \begin{bmatrix} 1 & \rho & \rho^2 & . & . & . & \rho^{N-1} \\ \rho & 1 & . & . & . & . & . \\ . & . & 1 & . & . & . & . \\ . & . & . & . & . & . & . \\ . & . & . & . & . & . & \rho^2 \\ . & . & . & . & . & . & \rho \\ \rho^{N-1} & . & . & . & . & \rho & 1 \end{bmatrix}$$

Спектр собственных значений является одним из основных средств для оценки эффективности алгоритмов сжатия изображений. Для определения спектра собственных значений сначала осуществляется БДЛВП корреляционной матрицы последовательности Маркова первого порядка, а потом вычисляются собственные значения вейвлет-коэффициентов W:

W =БДЛВП{ R }

$$\lambda = diag\{EingenValue(W)\}$$

Сравнительный анализ эффективности предложенного алгоритма по критерию компактности энергии вейвлет-функций представлен в табл. 2, используя два наибольших собственных значения спектра вейвлет-коэффициентов.

Таблица 2. **Оценка спектра собственных значений вейвлет-коэффициентов для вейвлет-функций с и без адаптации**

Уровень	Хаар	5/3	7/5	9/7	Бинарная	АЛВПК	АЛВПГ1D
1	1,0017	0,9961	9,1252	12,4724	1,7912	0,9667	6,2446
	6,2233	6,2318	1,4515	1,9117	6,5125	6,2209	0,9927
2	0,5864	0,5529	6,7496	12,6072	1,4409	0,4885	3,1638
	3,1257	3,1503	1,1463	1,7753	4,1742	3,1116	0,5320
3	0,5119	0,4077	5,1904	13,1280	1,3001	0,2372	1,6858
	1,5982	1,6748	0,9817	1,5090	3,3296	1,5599	0,4254
4	0,6025	0,7708	3,8211	13,1084	1,2914	0,1725	1,1989
	0,8566	0,8763	1,3954	1,7282	3,1564	0,7894	0,6516

Из табл. 2 видно, что эффективность использования вейвлет-функций БДЛВП по критерию компактности энергии на основе спектра собственных значений преобразованной корреляционной матрицы последовательности Маркова первого порядка превосходит вейвлет-функции Хаара и 5/3 без адаптации, АЛВПК и АЛВПГ приблизительно в 3 раза для четырех и выше уровней вейвлет-разложения. Однако не превосходит вейвлет-функции 7/5 и 9/7 без адаптации. Основными предмуществами БДЛВП является то, что оно не изменяет исходный динамический диапазон изображений в вейвлет-области и имеет положительные вейвлет-коэффициенты.

Заключение

Предложен алгоритм вычисления БДЛВП, основного для построения аппроксимационных и детализирующих бинарных фильтров, удовлетворяющих четыре основных ограничения на параметрах бинарных фильтров: ширину полосы пропускания, совершенное восстановление, количество нулевых моментов и перпендикулярность, которые гарантируют обратимости вейвлет-преобразований с требуемыми многомасштабными свойствами.

Данный алгоритм обеспечивает низкую вычислительную сложность, низкий объем бинарных промежуточных данных, отсутствие эффектов и ошибок квантования, а также отсутствие изменения в вейвлет-области исходного динамического диапазона изображений.

Из результатов моделирования следует, что предложенное БДЛВП обеспечивает увеличение концентрации энергии в минимальном количестве вейвлет-коэффициентов изображе-

ния по критерию оценки спектра собственных значений преобразованной корреляционной матрицы последовательности Маркова первого порядка, и по данному критерию превосходит в 3 раза некоторые стандартные и адаптивные вейвлет-функции.

AN ALGORITHM OF BINARY WAVELET TRANSFORM COMPUTATION BASED ON LIFTING SCHEME

L.A. RUIZ, A.A. BORISKEVICH

Abstract

An algorithm binary wavelet transform computation based on lifting-scheme, which provides low computational complexity, low binary intermediate data volume, the absence of quantization errors and dynamic original image range change in the wavelet-domain. Is required, this algorithm increases energy images concentration in a minimal amount of wavelet coefficients on criterion of the eigen value spectrum estimation of the transformed correlation matrix of the Markov sequence of first-order.

Литература

1. *Sweldens W.* // Proc. of SPIE. 1995. Vol. 2569. P. 68-79.
2. *Mallat S.* // IEEE Trans. Pattern Anal. Machine Intell. 1992. Vol. 14. P. 710-732.
3. *Parks T.* // Proc. IEEE Int. Conf. Acoust., Speech, Signal Processing, Albuquerque, NM. 1990. P. 2459-2462.
4. *Lewis A.* // IEEE Trans. Image Processing. 1992. Vol. 1. P. 244-250.
5. *Shapiro J.* // IEEE Trans. Signal Processing. 1993. Vol. 41. P. 3445-3462.
6. *Xu Y.* // IEEE Trans. Image Processing. 1994. Vol. 3. P. 747-758.
7. *Donoho D.* // Biometrika. 1994. Vol. 81. P. 425-455.
8. *Wornell G.* // IEEE Trans. Inform Theory. 1992. Vol. 38. P. 785-800.
9. *Freeland G.* // Proc. IEEE Int. Conf. Acoust., Speech, Signal Processing, Albuquerque, NM. 1990. P. 2345-2348.
10. *Moulin P.* // IEEE Trans. Signal Processing. 1994. Vol. 42. P. 3126-3136.
11. *Rioul O.* // IEEE Signal Processing Mug. 1991. Vol. 8. P. 14-38.
12. *Herley C.* // IEEE Trans. Signal Processing. 1993. Vol. 41. P 3341-3359.
13. *Tewfik A.* // Optic. Eng. 1994. Vol. 33. P. 2509-2519.
14. *Moulin P.* // IEEE Trans Inform. Theory. 1992. Vol. 38. P. 801-813.
15. *Swanson M.* // IEEE Transaction Image Processing. 1996. Vol. 5. P. 1637-1650.
16. *Vaidyanathan P.* // IEEE Int. Symp. Circuits Syst., New Orleans, LA, 1990. P. 1189-1192.
17. *Law N.* // Elsevier Signal Processing. 2007. Vol.87-11. P. 2850-2858.
18. *Law N.* // IEEE Image Processing, 2001. International Conference on Proceedings. 2001. Vol. 2. P. 281-284.
19. *Руис Л.* // Телекоммуникации: Сети и технологии. БГУИР. 2011. 26-32 с.
20. *Jain A.* // Fundamentals of Digital Image Processing. Prentice Hall Inc.1989.

УДК 004.056.55

РЕШЕНИЕ КВАДРАТНЫХ УРАВНЕНИЙ В ПОЛЯХ ГАЛУА ХАРАКТЕРИСТИКИ 2

В.А. БОГРЕЦОВ, В.А. ЛИПНИЦКИЙ

Белорусский Государственный Университет
пр-т. Независимости, 4, Минск, 220030, Беларусь

Военная академия Республики Беларусь
Минск-57, 220057, Беларусь

Поступила в редакцию 24 октября 2012

Рассматриваются 4 метода решения квадратных уравнений в полях Галуа характеристики 2. В частности, предлагается авторская версия метода неопределенных коэффициентов. Проводится сравнительный анализ эффективности рассматриваемых методов, на основе которого даются рекомендации по применению данных на практике.

Ключевые слова: поле Галуа, характеристика поля, нормальный базис поля, формула Ченя, БЧХ-код, синдром ошибки, норма синдрома.

Введение

Решение многих задач науки и техники так или иначе связано с решением алгебраических уравнений. Во второй половине XX века бурное развитие теории и практики защиты информации актуализировало необходимость решения уравнений над конечными полями, называемых также полями Галуа. К примеру, в помехоустойчивом кодировании поиск k-кратных ошибок сводится к решению алгебраического уравнения степени k над полями Галуа. Такие же задачи актуальны и в защите информации от несанкционированного доступа. В криптографических протоколах на основе эллиптических кривых постоянно решается задача нахождения корней квадратных уравнений над полями Галуа. Следует отметить, что существующие методы практического решения алгебраических уравнений вызывают нарекания у пользователей ввиду вязкости и громоздкости выполняемых при этом вычислений. Особенно отмеченная ситуация усугубляется над полями характеристики 2, где становятся бесполезными самые стандартные формулы и методы.

В работе подводится итог исследований, проводимых с последней четверти XX века, по разработке и анализу методов решения квадратных уравнений над полями Галуа.

Необходимые сведения о полях Галуа

Всякое поле Галуа характеристики 2 содержит в качестве минимального подполя поле $GF(2) \cong Z/2Z$, является конечномерным векторным пространством над $Z/2Z$ и, следовательно, состоит из 2^m элементов, где m – размерность данного векторного пространства. Как фактор-кольцо, $GF(2^m)$ состоит из полиномов вида $a_{m-1}\alpha^{m-1}+\ldots+a_1\alpha+a_0$, где $a_i \in Z/2Z$ и $\alpha = \bar{x}$ – элемент фактор-кольца, порожденный полиномом $x \in Z/2Z[x]$. $GF\left(2^m\right)$ – является расширением Галуа поля $GF(2)$, поскольку его группа $GF(2)$ автоморфизмов является циклической порядка m и порождена степенями автоморфизма Фробениуса $\varphi: x \to x^2$.

Важным для дальнейшего является понятие следа элемента конечного поля. Для произвольного $\gamma \in GF(2^m)$ его след $tr(\gamma) = \gamma + \varphi(\gamma) + \varphi^2(\gamma) + \ldots + \varphi^{2^{m-1}}(\gamma) = \gamma + \gamma^2 + \gamma^{2^2} + \ldots + \gamma^{2^{m-1}}$.

Ясно, что $tr(\gamma) \in GF(2)$. Как известно [1], что ровно половина элементов в $GF(2^m)$ имеет след 0 и половина имеет след 1. Операция следа является линейным оператором $GF(2^m) \to GF(2)$. Наиболее просто след вычисляется, если элемент γ задан в нормальном базисе [1]. Базис $GF(2)$ – пространства $GF(2^m)$ вида

$$\beta, \varphi(\beta), \varphi^2(\beta), \ldots, \varphi^{2^{m-1}}(\beta) \qquad (1)$$

называется нормальным. При этом $tr(\beta) = 1$. Существование таких базисов было доказано Дэвенпортом в 1968 году [2]. Если $\gamma = \gamma_0\beta + \gamma_1\varphi(\beta) + \gamma_2\varphi^2(\beta) + \ldots + \gamma_{m-1}\varphi^{2^{m-1}}(\beta)$, то $tr(\gamma) = \gamma_0 + \gamma_1 + \ldots + \gamma_{m-1}$.

Предварительные сведения о квадратных уравнениях

Наиболее общий вид квадратного уравнения: $Ax^2 + Bx + C = 0$, $A \neq 0$. Поделив уравнение на A, приходим к уравнению

$$x^2 + ax + b = 0. \qquad (2)$$

***Предложение* 1.** Уравнение (2) имеет в поле $GF(2^m)$ двукратный корень тогда и только тогда, когда $a = 0$. В этом случае $x_1 = x_2 = b^{1/2} = b^v$, где $v = 2^{m-1}$.

Отметим, что в [3] предложена оригинальная процедура вычисления $b^{1/2}$ в конкретных конечных полях характеристики 2. Случай уравнения (2), когда $b = 0$, легко решается: $x_1 = 0$, $x_2 = a$.

Далее будем считать, что в уравнении (2) коэффициенты a и b не равны нулю и принадлежат полю $GF(2^m)$. Такое уравнение имеет два различных корня либо в $GF(2^m)$, либо в его конечном расширении. В силу предложения 1, уравнение (2) нельзя привести к двучлену вида $x^2 + b = 0$. В полях характеристики 2 канонической формой уравнения (2) принято считать уравнение вида

$$t^2 + t + \gamma = 0 \qquad (3)$$

для некоторого $\gamma \in GF(2^m)$. Уравнение (2) приводится к виду (3) заменой $x = at$ [4]. При этом $\gamma = b / a^2$. Каноническая форма удобна тем, что если найден один корень t_1 уравнения (3), то второй корень получается автоматически: $t_2 = t_1 + 1$. Именно для канонического уравнения (3) имеет место критерий его разрешимости.

***Предложение* 2.** (Берлекэмп, Рамсей, Соломон) [5, 6]. Уравнение (2) над полем $GF(2^m)$ имеет корни в этом поле тогда и только тогда, когда $tr(\gamma) = 0$.

Формула и метод Ченя

***Предложение* 3.** (Чень) [7]. Пусть в уравнении (3) $tr(\gamma) = 0$, $\beta, \beta^2, \ldots, \beta^{2^{m-1}}$ – нормальный базис поля $GF(2^m)$ над $GF(2)$ и $\gamma = \gamma_0\beta + \gamma_1\varphi(\beta) + \gamma_2\varphi^2(\beta) + \ldots + \gamma_{m-1}\varphi^{2^{m-1}}(\beta)$. Тогда корень уравнения (3) $x_0 = \gamma_0\beta + (\gamma_0 + \gamma_1)\varphi(\beta) + (\gamma_0 + \gamma_1 + \gamma_2)\varphi^2(\beta) + \ldots + (\gamma_0 + \gamma_1 + \ldots + \gamma_{m-1})\varphi^{2^{m-1}}(\beta)$.

К сожалению, формула Ченя уже с виду выглядит достаточно громоздкой. Реальное ее применение сразу же наталкивается на проблему построения нормального базиса в поле $GF(2^m)$. На сегодняшний день, в общем случае, процедура поиска нормального базиса не имеет эффективного алгоритма и фактически является переборной: по очереди перебирают элементы поля $GF(2^m)$, для каждого из них составляют систему (1) и исследуют ее на линейную

зависимость. В [8] дана оценка количества нормальных базисов для поля $GF(p^m)$, согласно которой, с ростом m, вероятность нахождения нормального базиса за разумное время стремится к нулю. На практике наиболее часто используется стандартный базис $1,\alpha,\alpha^2,\ldots,\alpha^{m-1}$. Поэтому возникает необходимость перехода от полиномиального базиса к нормальному и обратно. Как отмечено в [9], сам Чень отчаялся найти упрощения в этом конгломерате вычислений, предложил отказаться от его формул и использовать для решения уравнения (3) метод последовательной подстановки элементов поля в это уравнение. Из уважения к его трудам, эта очевидная процедура носит название «метод Ченя».

***Замечание* 1.** Для применения на практике формулу Ченя можно несколько улучшить следующим образом. Пусть B – матрица перехода к нормальному базису, T – матрица, соответствующая преобразованию из формулы Ченя (очевидно, что оно линейно). Тогда формулу Ченя можно записать следующим образом $t = TB\gamma$. При этом, непосредственно из формулы Ченя и формулы следа элемента, заданного в нормальном базисе, следует, что t_{m-1} (коэффициент вектора t при $\varphi^{2^{m-1}}(\beta)$) будет являться следом γ. К примеру, над полем $GF(2^6)$ минимальное количество битовых операций, для перехода к нормальному базису и обратно равно 14, при этом еще необходимо выполнить 6 битовых операций в формуле Ченя, что в сумме дает 20 битовых операций. Минимальное же количество битовых операций, требуемых для решения уравнения (3), с использованием матрицы TB равно 16.

***Замечание* 2.** Не трудно заметить, что в поле $GF(2^m)$ в худшем случае для решения уравнения (3) по формуле Ченя с известной матрицей перехода к нормальному базису и известной матрицей для обратного перехода к полиномиальному базису требуется $2m^2 + m$ битовых операций: m^2 для перехода к нормальному базису, m непосредственно для самой формулы и m^2 для обратного перехода к полиномиальному базису. Если использовать оптимизацию из замечания 1, то требуется только $2m^2$ операций: m^2 для перехода к нормальному базису и m^2 для обратного перехода к полиномиальному базису. Таким образом, сложность решения уравнения (3) по формуле Ченя оценивается величиной $O(m^2)$ битовых операций.

Метод неопределенных коэффициентов

Альтернативой формулам Ченя является метод неопределенных коэффициентов, который опирается только на стандартный базис $1,\alpha,\alpha^2,\ldots,\alpha^{m-1}$.

Согласно *предложению* 2, если в уравнении (3) $tr(\gamma) = 0$, то его корни принадлежат полю $GF(2^m)$, над которым данное уравнение и рассматривается. Пусть t – один из корней уравнения (3). Как элемент поля $GF(2^m)$, его можно представить в виде $t = t_0 + t_1\alpha + \ldots + t_{m-1}\alpha^{m-1}$, $t_i \in GF(2)$. Подставим данное выражение t в уравнение (3). Получим соотношение: $\left(t_0 + t_1\alpha + \ldots + t_{m-1}\alpha^{m-1}\right)^2 + \left(t_0 + t_1\alpha + \ldots + t_{m-1}\alpha^{m-1}\right) + \gamma = 0.$ Так как в поле характеристики 2 выполняется равенство $(a+b)^2 = a^2 + b^2$ [1], то последнее соотношение преобразуется к виду:

$$\left(t_0 + t_1\alpha + \ldots + t_{m-1}\alpha^{m-1}\right)^2 + \left(t_0 + t_1\alpha + \ldots + t_{m-1}\alpha^{m-1}\right) + \gamma =$$
$$= {t^2}_0 + {t^2}_1\alpha^2 + \ldots + {t^2}_{m-1}\alpha^{2(m-1)} + t_0 + t_1\alpha + \ldots + t_{m-1}\alpha^{m-1} + \gamma.$$

где $t_i \in GF(2)$, поэтому $t_i^2 = t_i$, и последнее равенство будет эквивалентно следующему:

$$\gamma + t_0 + t_1\alpha^2 + \ldots + t_{m-1}\alpha^{2(m-1)} + t_0 + t_1\alpha + \ldots + t_{m-1}\alpha^{m-1} = 0. \qquad (4)$$

Согласно [1], $GF(2^m) \cong (Z/2Z)[x]/ < p(x) >$, где $p(x)$ – некоторый неприводимый над $Z/2Z[x]$ полином. После приведения равенства (4) по модулю $p(\alpha)$, получим уравнение относительно неизвестных $t_0, t_1, \ldots, t_{m-1}$:

$$\left(a_{m-1,m-1}t_{m-1}+\ldots+a_{m-1,1}t_1+a_{m-1,0}t_0\right)\alpha^{m-1}+\ldots+$$

$$+\left(a_{1,m-1}t_{m-1}+\ldots+a_{1,1}t_1+a_{1,0}t_0\right)\alpha+\left(a_{0,m-1}t_{m-1}+\ldots+a_{0,1}t_1+a_{0,0}t_0\right)+\gamma=0.$$

Так как система $1,\alpha,\ldots,\alpha^{m-1}$ линейно независима, то данное равенство равносильно системе уравнений

$$\begin{cases} a_{0\ 0}t_0+\ldots+a_{0\ m-1}t_{m-1}=\gamma_0 \\ a_{1\ 0}t_0+\ldots+a_{1\ m-1}t_{m-1}=\gamma_1 \\ \qquad\qquad \ldots \\ a_{m-1\ 0}t_0+\ldots+a_{m-1\ m-1}t_{m-1}=\gamma_{m-1} \end{cases}, \tag{5}$$

где $\gamma=\gamma_0+\gamma_1\alpha+\ldots+\gamma_{m-1}\alpha^{m-1}$. Далее для краткости будем называть систему (5) соответствующей уравнению (3).

***Предложение* 4.** Пусть над полем $GF(2^m)$ задано уравнение (3) и $At=\gamma$ – соответствующая ему система (5), записанная в матричном виде. Тогда матрица A может быть приведена элементарными преобразованиями строк к виду:

$$A'=\begin{bmatrix} 0 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{bmatrix}.$$

Доказательство. Так как γ не влияет на матрицу A, то можно ограничиться рассмотрением уравнения

$$t^2+t=0 \tag{6}$$

Очевидно, 0 является решением этого уравнения. Так как характеристика поля равна 2, то 1 также является решением. Согласно теореме Безу, квадратное уравнение может иметь не больше двух корней и, следовательно, других решений уравнение (6) иметь не может. Система (5) для уравнения (6) будет однородной. Ее решениями будут вектора $(0,0\ldots,0)$, $(1,0\ldots,0)\in(Z/2Z)^m$. Следовательно, фундаментальная система решений будет иметь вид $(\tau,0,\ldots,0)$, $\tau\in Z/2Z$. Но это означает, что базисный минор матрицы A системы (5) для уравнения (6) расположен в столбцах с номерами $2,\ldots,m$, поэтому матрицу A можно элементарными преобразованиями строк привести к требуемому виду.

***Следствие* 1.** Пусть задано уравнение (3) над полем $GF(2^m)$ и $At=\gamma$ – соответствующая ему система (5). Пусть далее $S_1,\ldots,S_n\in M_m(Z/2Z)$ – элементарные матрицы, соответствующие элементарным преобразованиям строк, приводящим матрицу A к A', $S=S_1S_2\ldots S_n$, $\gamma'=S\gamma$. При этом $\gamma',\gamma'+1$ – корни уравнения (3) тогда и только тогда, когда $\gamma'_0=0$, где

$$\gamma'=\gamma'_0+\gamma'_1\alpha+\ldots+\gamma'_{m-1}\alpha^{m-1}.$$

Тогда, если $\gamma'_0=1$, то уравнение не имеет решений.

Доказательство. Достаточно записать систему $SAt=A't=S\gamma=\gamma'$ в явном виде

$$\begin{cases} 0 = \gamma'_0 \\ t_1 = \gamma'_1 \\ \cdots \\ t_{m-1} = \gamma'_{m-1} \end{cases}.$$

Из предложения 2 вытекает

***Следствие* 2.** Из предложения 2 и следствия 1 вытекает следующее утверждение:

$\forall \gamma \in GF(2^m) \quad tr(\gamma) = \gamma'_0$.

Замечание 3. Очевидно, для решения квадратных уравнений над заданным полем не обязательно вычислять матрицу S каждый раз. Она может быть вычислена однажды для конкретного $p(x)$ и затем использоваться для решения уравнения (3) с произвольным γ.

***Замечание* 4.** Не трудно заметить, что решение уравнения (3) в поле $GF(2^m)$ методом неопределенных коэффициентов с известной матрицей S в худшем случае требует m^2 битовых операций. Таким образом, метод неопределенных коэффициентов для решения уравнения (3) имеет сложность в худшем случае $O(m^2)$.

Пример 1. Рассмотрим поле $F = GF\left(2^5\right) = (Z/2Z)[x]/ < 1 + x^2 + x^5 >$. Система (5) для уравнения (6) в этом поле имеет матрицу

$$A = \begin{bmatrix} 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 \end{bmatrix}.$$

Непосредственные вычисления показывают, что в данном случае

$$S = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \end{bmatrix}.$$

Рассмотрим над полем F квадратное уравнение $t^2 + t + 1 + \alpha + \alpha^2 + \alpha^3 + \alpha^4 = 0$. Для этого уравнения $\gamma = (1,1,1,1,1)$ и

$$S\gamma = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 1 \end{bmatrix} = \gamma'.$$

Здесь $tr(\gamma) = \gamma'_0 = 0$, следовательно, $t_1 = \alpha^3 + \alpha^4$, $t_2 = 1 + \alpha^3 + \alpha^4$ – решения уравнения

$t^2 + t + 1 + \alpha + \alpha^2 + \alpha^3 + \alpha^4 = 0$.

Пример 2. Рассмотрим над полем из примера 1 уравнение $t^2 + t + 1 + \alpha + \alpha^2 + \alpha^4 = 0$. Для этого уравнения матрица S будет та же, что и в примере 1, $\gamma = (1,1,1,0,1)$:

$$S\gamma = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \\ 1 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix} = \gamma'$$

$tr(\gamma) = \gamma'_0 = 1$, следовательно, данное уравнение в поле F решений не имеет.

***Замечание* 5.** В некоторых случаях может быть более эффективным не вычисление произведения $S\gamma$, а применение к γ преобразований, соответствующих матрице S. В этом можно убедиться, рассмотрев поле $(Z/2Z)[x]/<1+x^2+x^3+x^4+x^8>$.

Ниже в табл. 1 приводится сравнение производительности решения уравнения (3) в поле $GF(2^m)$ в полиномиальном базисе по формуле Ченя (с оптимизацией из замечания 3) и методом неопределенных коэффициентов.

Таблица 1. **Сравнение эффективности формулы Ченя и метода неопределенных коэффициентов**

m	n_1	$p_1(x)$	n_2	$p_2(x)$
4	8	$1+x+x^4$	4	$1+x+x^4$
5	14	$1+x^2+x^5$	5	$1+x^3+x^5$
6	15	$1+x+x^6$	7	$1+x+x^6$
7	31	$1+x+x^2+x^3+x^4+x^5+x^7$	9	$1+x^3+x^7$
8	33	$1+x^3+x^5+x^7+x^8$	14	$1+x^2+x^3+x^4+x^8$
9	33	$1+x+x^4+x^5+x^6+x^8+x^9$	12	$1+x^5+x^9$

В табл. 1 n_1 – количество битовых операций, требуемых для решения уравнения (3) по формуле Ченя в поле $(Z/2Z)[x]/<p_1(x)>$, p_1 – примитивный многочлен, по которому строится поле, в котором решение уравнения (3) по формуле Ченя оптимально среди остальных примитивных многочленов над $Z/2Z$ такой же степени, n_2 – количество битовых операций, требуемых для решения уравнения (3) методом неопределенных коэффициентов в поле $(Z/2Z)[x]/<p_2(x)>$, p_2 – примитивный многочлен, по которому строится поле, в котором решение уравнения (3) методом неопределенных коэффициентов оптимально среди остальных примитивных многочленов над $Z/2Z$ такой же степени. Из табл. 1 и *замечаний* 2 и 4 видно, что метод неопределенных коэффициентов имеет более высокую эффективность для решения квадратных уравнений в полях Галуа характеристики 2, чем метод, основанный на формуле Ченя.

***Замечание* 6**. В [6] над полями $GF(2^m)$ с нечетным m рассмотрено применение метода неопределенных коэффициентов, приводящее к более громоздким вычислениям.

Норменный метод

В [4] предложен довольно нестандартный метод решения уравнения (2), при котором даже не требуется переход к уравнению (3). Суть его заключается в тесной связи между уравнениями над $GF(2^m)$ и двоичными БЧХ-кодами [3]. Известно [3], что декодирование БЧХ-кодов C_{2t+1}, способных исправлять t-кратные ошибки, сводится к решению алгебраического уравнения степени t над полем Галуа. В [10] разработана теория норм синдромов, позволяющая не прибегать к решению уравнений для декодирования БЧХ-кодов. Согласно [4], норма синдрома для двоичного БЧХ-кода C_5 длиной $n = 2^m - 1$, исправляющего двойные ошибки, определяется как величина $N = s_2 / s_1^3 \in GF(2^m)$, где (s_1, s_2) – синдром принятого сообщения. Алгоритм декодирования такого кода норменным методом заключается в следующем [4].

1. Строится список $T=\{N_0,N_1,\ldots,N_\theta\}$, где $N_i=N(e_i)$ – норма образующей вектор-ошибки [10] $e_i=(1,i)$, $0\le i\le\theta=2^{m-1}-1$.

2. Вычисляется синдром $S=(s_1,s_2)$, $s_1,s_2\in GF(2^m)$ очередного принятого сообщения.

3. Если $S=(s_1,s_2)\neq\bar{0}$, вычисляется норма данного синдрома $N=N(S)=s_2/s_1^3$.

4. Находится номер k полученного значения N в списке T, для которого $N_k=N$. Соответствующей ему образующей вектором-ошибкой будет $e_k=(1,k)$.

5. Вычисляется $s_1/s_1^k=\alpha^\mu\in GF(2^m)$, $0\le\mu\le 2^m-1$, α – примитивный элемент поля $GF(2^m)$.

6. При помощи найденного значения μ вычисляется $e=\sigma^\mu(e_k)=(t_1,t_2)$ – искомый вектор ошибки, где t_1,t_2 – локаторы ошибочных позиций, σ – оператор циклического сдвига вправо.

***Замечание* 7.** Для применения на практике норменного метода декодирования БЧХ-кода список T из пункта 1 достаточно вычислить однажды и сохранить в ПЗУ декодирующего устройства. Таким образом, нахождение ошибочных позиций в принятом сообщении сводится буквально к нескольким арифметическим операциям в поле Галуа.

Опишем теперь, как можно применить норменный метод для решения квадратных уравнений в конечном поле характеристики 2. Пусть над полем $GF(2^m)$ задан двоичный БЧХ-код C_5 длиной $n=2^m-1$. Пусть $S=(s_1,s_2)$ – синдром принятого сообщения, $s_1,s_2\in GF(2^m)$. Согласно [4], если $x=\alpha^u$, $y=\alpha^v\in GF(2^m)$ [4], α – примитивный элемент поля $GF(2^m)$ удовлетворяют следующей системе уравнений:

$$\begin{cases} x+y=s_1,\\ x^3+y^3=s_2. \end{cases}$$

то $u+1, v+1$ – номера ошибочных позиций в принятом сообщении. Так как $x^3+y^3=(x+y)(x^2-xy+y^2)=s_1(s_1^2+xy)=s_2$, то исходная система может быть преобразована к более простому виду

$$\begin{cases} x+y=s_1,\\ xy=s_1^2+s_2/s_1. \end{cases}$$

Данная система, исходя из формул Виета, эквивалентна следующему квадратному уравнению $t^2+s_1t+s_1^2+s_2/s_1=t^2+at+b=0$ над полем $GF(2^m)$. Так как корни данного уравнения являются локаторами ошибочных позиций, соответствующих синдрому (s_1,s_2), то, с учетом выше приведенного метода декодирования, получаем следующий алгоритм решения уравнения (2) [4].

1. Вычисляется $N=1+b/a^2$.

2. В списке T находится $N_k=N$.

3. $t_1=a/(1+\alpha^{k+1})$.

4. $t_2=t_1\alpha^{k+1}$.

Пример 3. Решим норменным методом уравнение из примера 1 над тем же полем. В данном случае список T будет иметь следующий вид

Таблица 2. **Показатели норм синдромов двойных ошибок примитивного БЧХ-кода с $n=31$**

i	1	2	3	4	5	6	7	8	9	10	11	12	13	14
$degN_i$	12	22	24	18	13	21	17	20	5	10	26	9	11	3

В соответствии с предложенным алгоритмом, вычислим норму

$$N = 1 + \frac{b}{a^2} = 1 + 1 + \alpha + \alpha^2 + \alpha^3 + \alpha^4 = \alpha + \alpha^2 + \alpha^3 + \alpha^4 = \alpha^{24}.$$

В табл. 2 $deg N_3 = 24$, следовательно, $k = 3$. Поэтому $t_1 = a/(1+\alpha^4) = 1/(1+\alpha^4) = \alpha^3 + \alpha^4$, $t_2 = (\alpha^3 + \alpha^4)\alpha^4 = 1 + \alpha^3 + \alpha^4$.

При многократном решении квадратных уравнений (2) над полем $GF(2^m)$, норменный метод демонстрирует наибольшую простоту и эффективность применения.

Заключение

Проведено исследование и дана сравнительная оценка четырех основных методов решения квадратных уравнений над полями Галуа характеристики 2. Следует, что формула Ченя имеет скорее теоретическое значение для решения данной задачи. Для практического же применения более эффективными являются метод неопределенных коэффициентов и, особенно, норменный метод. Последний, в свою очередь, может применяться для уравнений более высоких степеней в полях произвольной положительной характеристики и поэтому представляет особенный интерес для дальнейшего изучения.

SOLVING OF QUADRATIC EQUATIONS OVER FINITE FIELDS OF CHARACTERISTIC 2

V.A. BOGRETSOV, V.A. LIPNITSKI

Abstract

There are four solving methods of quadratic equations over Galois finite fields of characteristic 2 considered in this article. Particularly it is proposed to get acquainted with the author`s version of the undetermined coefficients method. There is a contrastive analysis of considered methods efficiency, on which basis are given recommendations to practice the data.

Литература

1. *Лидл Р., Нидеррайтер Г.* Конечные поля. М., 1988.
2. *Davenport H.* // J. London Math. Soc. 1968. Vol. 43. P. 21-39.
3. *Берлекэмп Э.* Алгебраическая теория кодирования. М., 1971.
4. *Липницкий В.А., Конопелько В.К.* Норменное декодирование помехоустойчивых кодов и алгебраические уравнения. Мн., 2007.
5. *Berlekamp E.R.* // Info. and Control. 1967. Vol. 10. P. 553-564.
6. *Болотов А.А., Гашков С.Б., Фролов А.Б.* Элементарное введение в эллиптическую криптографию. Протоколы криптографии на эллиптических кривых. М., 2012.
7. *Chen C.L.* // IEEE Trans. of inf. Theory. 1982. Vol. 28, №5. P. 792-794.
8. *Болотов А.А., Гашков С.Б., Фролов А.Б. и др.* Элементарное введение в эллиптическую криптографию. Алгебраические и алгоритмические основы. М., 2012.
9. *Муттер В.М.* Основы помехоустойчивой телепередачи информации. Л., 1990.
10. *Конопелько В.К., Липницкий В.А.* Теория норм синдромов и перестановочное декодирование помехоустойчивых кодов. М., 2004.

УДК 004.056.5:519.254

СИСТЕМА СТАТИСТИЧЕСКОГО ТЕСТИРОВАНИЯ ГЕНЕРАТОРОВ СЛУЧАЙНЫХ ЧИСЕЛ ЭЛЕКТРОННЫХ ПЛАСТИКОВЫХ КАРТ

Н.Г. КИЕВЕЦ, А.И. КОРЗУН

Белорусский государственный университет информатики и радиоэлектроники
П. Бровки, 6, Минск, 220013, Беларусь

Поступила в редакцию 3 мая 2012

Рассматриваются системы статистического тестирования генераторов случайных чисел. Предлагается система статистических тестов для генераторов случайных чисел электронных пластиковых карт.

Ключевые слова: электронная пластиковая карта, генератор случайных чисел, статистические тесты.

Введение

Современные информационные технологии передачи данных строятся с обязательным использованием личного идентификатора, в качестве которого наиболее целесообразно использовать электронные пластиковые карты (ЭПК) в различных форм-факторах.

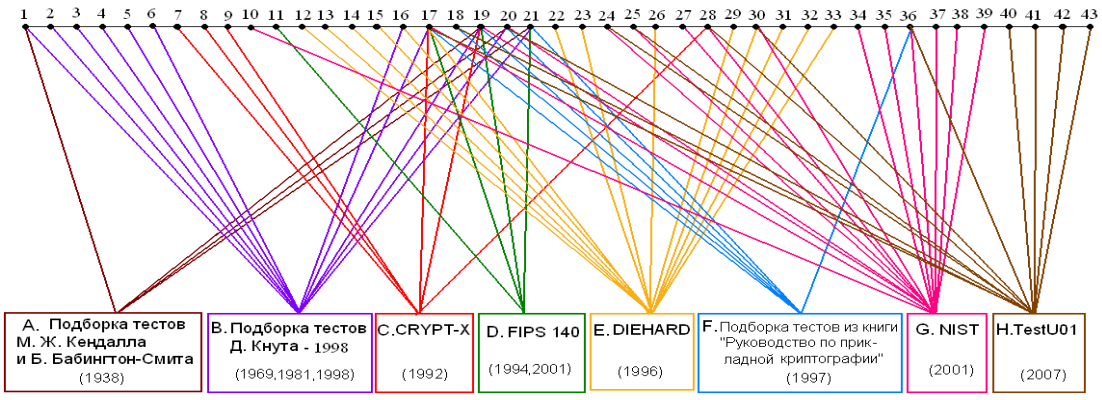
Особенностью ЭПК является наличие в их составе генераторов случайных чисел (ГСЧ), на основе которых вырабатываются ключи шифрования. Качество работы ГСЧ определяет качество ключей, а в целом криптостойкость передаваемых данных. Поэтому представляет интерес выбор и формирование системы тестов, с помощью которой целесообразно оценивать качество работы ГСЧ карт различных производителей.

Целью данной работы является рассмотрение существующих систем статистических тестов и формирование системы тестов для оценки качества работы ГСЧ.

Анализ подборок статистических тестов для оценки качества работы ГСЧ

В связи с большим объемом информации, описывающей каждый из тестов, в данной работе не приводится математического описания каждого из тестов. Тем не менее, ясно, что каждый тест представляет собой набор процедур.

На рисунке представлены наиболее известные подборки статистических тестов для исследования качества работы генераторов случайных чисел.



Подборки статистических тестов

Расшифровка тестов приведена ниже.

1. Тест интервалов (Gap test).
2. Тест конфликтов (Collision test).
3. Тест «максимум t» (Maximum-of-t test).
4. Тест сериальной корреляции (Serial correlation test).
5. Тест собирателя купонов (Coupon collector's test).
6. Тест перестановок (Permutation test).
7. Проверка бинарной производной (Binary derivative test).
8. Тест точек перехода (Change point test).
9. Тест сложности последовательности (Sequence complexity test).
10. Проверка кумулятивных сумм (Cumulative sums (Cusum) test).
11. Тест длинных подпоследовательностей (Long run test).
12. Тест на парковку (Parking lot test).
13. Обезьяньи тесты (Monkey tests).
14. Тест сжатия (Squeeze test).
15. Тест 3D-сфер (3D spheres test).
16. Тест промежутков между днями рождения (Birthday spacings test).
17. Тест подпоследовательностей (Run test или Runs test).
18. Проверка автокорреляции (Autocorrelation test).
19. Частотный тест (Frequency test).
20. Тест серий (Serial Test).
21. Тест покера (Poker test).
22. Тест пересекающихся сумм (Overlapping sums test).
23. Тест игры в кости (Craps test).
24. Спектральный тест (Spectral test).
25. Проверка сжатия при помощи алгоритма Лемпель-Зива (Lempel-Ziv complexity test или Lempel-Ziv compression test).
26. Подсчет числа единиц в определенных байтах (Count the 1's in specific bytes).
27. Проверка аппроксимированной энтропии (Approximate entropy test).
28. Проверка линейной сложности (Linear complexity test).
29. Проверка потока бит (Bitstream test).
30. Проверка рангов матриц (Binary matrix rank test).
31. Подсчет 1 в потоке байт (The count-the-1's test on a stream of byte).
32. Тест на минимальное расстояние (Minimum distance test).
33. Проверка пересекающихся перестановок (Overlapping 5-permutations test).
34. Частотный тест в подпоследовательностях (Frequency test within a block).
35. Проверка случайных отклонений (Random excursion test).
36. Универсальный тест Маурера (Maurer's «Universal Statistical» test).
37. Тест «блоков» в подпоследовательностях (Test for longest run of ones in a block).
38. Проверка пересекающихся шаблонов (Overlapping template matching test).
39. Проверка непересекающихся шаблонов (Non-overlapping template matching test).
40. Проверка случайных блужданий (Random walk test).
41. CAT-тест (CAT-test).
42. Проверка весов Хэмминга (Hamming weights).
43. Тест самой длинной последовательности (Longest run of 1's test).

Анализ наиболее часто употребляемых тестов, приведенных на рисунке, дает возможность увидеть, что тест подпоследовательностей 17 включен в 7 из 8 систем тестирования, частотный тест 19 входит в 6 из 8 приведенных систем, тест серий 20 содержится в 5 системах тестирования, тест покера 21 – в 4 системах. Все подборки содержат, по крайней мере, один из четырех перечисленных тестов. Данные тесты принято считать базовыми. Они использовались для исследования первых механических, физических и программных генераторов случайных чисел и используются в существующих системах тестирования, что подтверждается рисунком.

Первая подборка статистических тестов для оценки качества ГСЧ был опубликована в 1938 году М.Ж. Кендаллом и Б. Бабингтон-Смитом, которые предложили использовать четыре теста [1]: частотный тест, тест серий, тест покера и тест интервалов. Данные тесты являются

базовыми и включены в большинство существующих подборок тестов. Тесты были описаны для последовательностей десятичных чисел от 0 до 9, так как предназначались для оценки качества работы механических генераторов. На рисунке видно, что тест интревалов содержится еще лишь в подборке Д. Кнута. Однако, при использовании битовых последовательностей тест интервалов можно считать тестом подпоследовательностей. Действительно, интервал между единицами есть подпоследовательность нулей. В работе [2] подборка тестов М.Ж. Кендалла и Б. Бабингтон-Смита рассмотрена для случая битовых последовательностей.

Фундаментальной работой, на которую ссылаются большинство разработчиков статистических тестов, является второй том книги Д. Кнута «Искусство программирования» (The Art of Computer Programming) [3-5]. В нем представлена подборка тестов, которые традиционно применяются для исследования статистических свойств псевдослучайных последовательностей. Некоторые тесты рассмотрены для целочисленных последовательностей, а некоторые для последовательностей действительных чисел, принадлежащих интервалу (0;1). Тесты, описанные для последовательности чисел, принадлжащие интервалу (0;1), могут быть использованы также и для исследования битовых последовательностей. Например, в работе [6] тест интервалов подборки Д. Кнута описан для битовых последовательностей. Подборка Д. Кнута содержит все четыре теста набора М.Ж. Кендалла и Б. Бабингтон-Смита. В работе [6] отмечаются следующие недостатки подборки тестов Д. Кнута.

1. Отсутствие рекомендуемых параметров тестирования. Не совсем корректный выбор некоторых значений может привести к тому, что ряд тестов будет зависеть от длины исследуемой последовательности или браковать все последовательности.

2. Спорная методика оценки результатов. Д. Кнут предлагает считать последовательности, для которых вероятность появления данного результата лежит в интервалах [0;0,01] и [0,99;1], неслучайными, (0,01;0,1] и [0,9;0,99) – подозрительными на случайность, (0,1;0,9) – случайными. Таким образом, для истинно случайной последовательности вероятность должна стремиться к 0,5, хотя, как представляется, на самом деле она должна стремиться к 0.

Пакет статистических тестов Crypt-X [7] разработан исследовательским центром информационной безопасности Квинслендского университета технологий. Три из шести тестов являются распространенными и входят в подборки: тест 17 в подборки B, D, E, F, G и H, тест 19 входит в подборки A, B, F и G, тест 28 включен также в подборки G и H. Три теста не содержатся в других подборках.

Стандарт FIPS 140-1 [8] содержит четыре статистических теста, три из которых считаются базовыми (частотный тест, тест подпоследовательностей, тест покера) и тест длинных подпоследовательностей. Данную подборку можно использовать для контроля генераторов, но она малопригодна для статистической оценки генераторов. Более поздняя версия стандарта – FIPS 140-2 [9] содержит те же 4 теста, но с измененными диапазонами допустимых значений тестовых статистик. Недостатком подборки FIPS 140-1 является то, что для тестирования требуется непрерывная последовательность длиной 20000 бит. ГСЧ ЭПК не позволяет получить непрерывную последовательность такой длины.

Тесты DIEHARD были опубликованы в 1996 году на CD-ROM [10]. Система тестов DIEHARD предназначена для битовых последовательностей. Для некоторых тестов битовая последовательностей преобразуется в последовательность чисел, принадлежащих интервалу (0;1). В работе [6] авторы выделены следующие недостатки системы DIEHARD.

1. Описания некоторых тестов (а именно a parking lot test, the minimum distance test, 3Dspheres test, the squeeze test, the overlapping sums, the runs test и the craps test), не позволяют понять смысл этих тестов.

2. Параметры тестирования жестко заданы, например, размер области тестирования – независимо от размера файла анализируется определенное число байт.

3. Полностью отсутствует справочная служба и методика трактовки результатов.

4. Большинство тестов основано не на теоретических расчетах, а на результатах испытаний.

В работе [11] содержатся пять базовых тестов (частотный тест, тест серий, тест покера, тест подпоследовательностей и проверку автокорреляции), к которым добавлен универсальный тест Маурера. Отмечено, что тест Маурера может находить все отклонения от случайности, ко-

торые находят пять базовых тестов, но тест Маурера требует гораздо более длинных последовательностей.

Подборка тестов NIST [12] содержит 16 тестов. Система NIST содержит как базовые тесты, так и другие более мощные тесты, некоторые из которых включены в более ранние подборки (например, тест Маурера).

TestU01 [13] представляет собой библиотеку программ, предназначенных для статистического тестирования генераторов случайных равномерно распределенных чисел. Библиотека состоит из четырех модулей. Один из модулей содержит набор статистических тестов, в который включены классические тесты, другие тесты, приведенные в литературе, и несколько оригинальных тестов. Другой модуль библиотеки содержит шесть определенных подборок тестов. Три подборки предназначены для тестирования последовательностей действительных случайных чисел, равномерно распределенных на интервале (0;1). Три подборки предназначены для битовых последовательностей: Rabbit, Alphabit и Block Alphabit. Rabbit и Alphabit содержат 38 и 17 тестов соответственно. Подборка Block Alphabit предназначена для последовательностей, состоящих из блоков различной длины. Авторы подборок не утверждают, что подборки содержат независимые тесты, которые выявляют все возможные отклонения от случайности. Они считают, что трудно проверить независимость тестов и сравнить их эффективность. Тесты для подборок были выбраны в основном благодаря распространенности использования. В публикации [13] описаны некоторые тесты, содержащиеся в библиотеке TestU01 (отмечены на рисунке), но не приведены определенные перечни тестов, входящих в тестовые подборки.

Таким образом, рассмотрены восемь наиболее широко описанных в литературе подборок тестов. Существует система базовых тестов, входящих практически во все подборки. Система базовых тестов дополняется в каждой подборке своими специфическими тестами, отличающими одну подборку от другой.

Подборка тестов для оценки качества ГСЧ ЭПК

При выборе статистических тестов для оценки качества ГСЧ ЭПК необходимо учитывать следующие особенности:

- ГСЧ ЭПК являются физическими генераторами;
- ГСЧ ЭПК не вырабатывают непрерывную последовательность бит, а выдают случайные числа определенных длин.

Для эффективного тестирования необходимо использовать набор тестов, которые должны удовлетворять следующим условиям.

1. Тесты набора должны находить все возможные виды отклонений от случайности.
2. Тесты должны быть независимыми. Не следует использовать тестов больше, чем это необходимо.

Подборки М.Ж. Кендалла и Б. Бабингтон-Смита и FIPS 140 содержат тесты, которые широко распространены и считаются базовыми. Достоинством данных тестов является то, что для тестирования не требуется последовательностей большой длины. Использование тестов только данных подборок позволяют сделать предварительную оценку качества работы ГСЧ. Их целесообразно дополнить более сложными тестами, выявляющими широкий спектр аномалий в исследуемой последовательности.

Недостатки подборки Д. Кнута (отсутствие рекомендуемых параметров тестирования, спорная методика оценки результатов тестирования) требуют дополнительных доказательств применимости данной системы тестов для оценки качества работы ГСЧ ЭПК.

Пакет статистических тестов Crypt-X содержит три широкоупотребимых теста (частотный тест, тест подпоследовательностей, проверка линейной сложности), которые в том числе включены в систему NIST. Тест бинарной производной подборки Crypt-X в сущности является эквивалентом теста серий в случае пересекающихся серий. Тест сложности последовательности разработан для замены теста автокорреляции. Тест точек перехода предусматривает приближенное вычисление вероятности, погрешность которого не описана.

Подборка тестов из книги «Руководство по прикладной криптографии» практически входит в состав системы NIST.

Учитывая, что ГСЧ ЭПК не позволяет получить непрерывную битовую последовательность, следовало бы использовать подборку тестов для исследования последовательностей чи-

сел различной длины. Тесты DIEHARD предназначены исключительно для последовательностей чисел длиной 32 бита. Подборка тестов Block Alphabit из программной библиотеки TestU01 предназначена для исследования последовательностей, состоящих из блоков различной длины (2, 4, 8, 16 и 32 бита). Некоторые карты позволяют получить последовательность длиной 1-9, 16-25, 32 (ОСКАР), 48, 64, 80, 96, 112, 128,144 (MINOS) байта. Поскольку отсутствует четкое описание всех содержащихся в данных программах тестов, представляется сложным доказать правомерность их использования для тестирования карт ОСКАР и MINOS.

Система NIST практически лишена недостатков, присущих описанным выше системам. Кроме того, она обладает следующими достоинствами.

1. Данная подборка получила широкое распространение.
2. Все тесты предназначены для оценки битовых последовательностей.
3. Система включает в себя достаточно большое количество тестов – 16.
4. Тесты системы являются примерно независимыми [14].
5. Имеется подробное описание тестов с примерами и рекомендуемыми параметрами.
6. Система тестов создана относительно недавно – в 2001 году и вобрала в себя практически все достижения в области статистического тестирования ГСЧ.

В связи с вышеперечисленными достоинствами система NIST была взята за основу при создании системы тестирования ГСЧ ЭПК. Вследствие специфики ГСЧ ЭПК из системы NIST исключен тест 25, так как для тестирования необходимо знать параметры, которые не определяются теоретически. Эти значения получают, используя генератор с функцией SHA-1 в цепи обратной связи или генератор Blum-Blum-Shub.

Поскольку тест «Стопка книг» может эффективнее находить отклонения от случайности, чем тесты NIST [15], целесообразно сформировать систему тестов с учетом включения в нее теста «Стопка книг». Кроме того, при использовании данного теста последовательность разбивается на блоки, длина которых хорошо согласуется с длиной ключа, вырабатываемого ГСЧ ЭПК.

Таким образом, в окончательном виде система статистических тестов для оценки качества работы ГСЧ ЭПК состоит из тестов 10, 17, 19, 20, 24, 25, 27, 28, 30, 34, 35, 36, 37, двух вариантов теста 39 (см. рисунок) и теста «Стопка книг».

Заключение

Предложена система статистических тестов для генераторов случайных чисел электронных пластиковых карт. Система базируется на шестнадцати тестах, четыре из которых широко используются в других системах тестирования. Обосновывается использование тестов в предложенной системе тестирования.

STATISTICAL TESTING SYSTEM FOR PLASTIC CARDS RANDOM NUMBER GENERATORS

N.G. KIYEVETS, A.I. KORZUN

Abstract

The statistical testing system for plastic cards random number generators are considered. The system of statistical tests for plastic cards random number generators is offered.

Литература

1. *Kendall M.G.* // Journal of the Royal Statistical Society. 1938. Vol. 101, №1. P. 147-166.
2. *Isakson H.A.* // Generator of Random Numbers – Teleteknik. 1959.Vol. III, №2.
3. *Donald E. Knuth* // The Art of Computer Programming. 1969.
4. *Donald E. Knuth* // The Art of Computer Programming. 1981.
5. *Donald E. Knuth* // The Art of Computer Programming. 1998.
6. *Иванов М.А., Чугунков И.В.* Теория, применение и оценка качества генераторов псевдослучайных последовательностей. М., 2003.
7. *Caelli W., Dawson E., Nielsen L.* // CRYPT–X Statistical Package Manual, Measuring the Strength of Stream and Block ciphers. 1992.
8. Federal Information Processing Standards Publication 140-1. «Security Requirements for Cryptographic Modules» U.S. Department of Commerce/NIST. 1994.
9. Federal Information Processing Standards Publication 140-2. «Security Requirements for Cryptographic Modules» U.S. Department of Commerce/NIST. 2001.
10. *Marsaglia G.* // The Marsaglia Random Number CDROM including the DIEHARD Battery of Tests of Randomness. 1996.
11. *Alfred J. Menezes, Paul C. Van Oorschot, Scott A. Vanstone* Handbook of Applied Cryptography. 1997.
12. *L'Ecuyer P., Simard R.* // Library for Empirical Testing of Random Number Generators. – ACM Transactions on Mathematical Software. 2007. Vol. 33. P. 32.
13. *Soto J.* // Proceedings of the 22nd National Information Systems Security Conference. 1999.
14. *Миненко А.И.* // Вестник СибГУТИ. 2010. №4. С. 36-46.

УДК 621.315.4/.61

ВЛИЯНИЕ ДОБАВОК БИШОФИТА НА ХАРАКТЕРИСТИКИ ПИРАМИДООБРАЗНЫХ ЭКРАНОВ ЭЛЕКТРОМАГНИТНОГО ИЗЛУЧЕНИЯ ДЛЯ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ И ЭКОЛОГИЧЕСКОЙ БЕЗОПАСНОСТИ

М.Ш. МАХМУД, Е.С. БЕЛОУСОВА, А.М. ПРУДНИК, Л.М. ЛЫНЬКОВ

Белорусский государственный университет информатики и радиоэлектроники
П. Бровки, 6, Минск, 220013, Беларусь

Поступила в редакцию 2 мая 2012

Предложено использование порошковых бишофита и шунгита для создания поглотителей электромагнитного излучения. Представлены результаты исследования характеристик ослабления и отражения электромагнитного излучения в диапазоне частот 0,5… 18 ГГц углеродосодержащими пирамидообразными экранами с добавлением бишофита.

Ключевые слова: бишофит, шунгит, экранирующие свойства.

Введение

Защита организма человека от воздействия электромагнитных излучений предполагает снижение их интенсивности до уровней, не превышающих предельно допустимые. Защита обеспечивается выбором конкретных методов и средств, учетом их экономических показателей, простотой и надежностью эксплуатации. Спектр излучения компьютера включает в себя рентгеновскую, ультрафиолетовую и инфракрасную области спектра, а также широкий диапазон электромагнитных волн других частот. Опасность рентгеновских лучей считается сейчас специалистами пренебрежимо малой, поскольку этот вид лучей поглощается веществом экрана. В отличие от ионизирующего излучения низкочастотные излучения не могут расщеплять или ионизировать атомы, и раньше считалось, что неионизирующее излучение не может негативно воздействовать на организм, если оно недостаточно сильно, чтобы вызвать тепловые эффекты или электрический шок [1].

Эксперимент

Для обеспечения защиты информации предлагается использовать материалы с добавлением углеродсодержащих материалов, поэтому целью исследования является разработка растворных смесей на основе шунгита и бишофита и исследование их экранирующих свойств (коэффициентов отражения и ослабления) [2].

Материалы, поглощающие электромагнитное излучение (ЭМИ) используются как при строительстве и отделке помещений, так и для создания разборных модульных конструкций [3]. Основными принципами экранирования являются перенаправление энергии электромагнитных волн за счет отражения от поверхностей материалов, а также поглощение волн внутри них [4].

Бишофит – это кристаллическая соль, образовавшаяся на глубине 12,5 км более 200 миллионов лет назад при испарении морей. В ископаемом состоянии бишофит встречается в виде соляной зернисто-кристаллической породы. В чистом виде кристаллы бишофита водянопрозрачные, но могут иметь белую, розовую и бурую окраску в зависимости от примесей. В состав бишофита входят около 70 химических элементов, в том числе, хлорид магния (главное действующее вещество), а также йод, бром, железо, кремний, цинк и др.

Для изучения влияния геометрии поверхности экрана на его характеристики ослабления и отражения электромагнитых волн разработана технология создания шунгитобетонных монолитных модулей с добавлением бишофита. В качестве подложки использовали промышленно производимые прессованием целлюлозные формы, используемые для транспортировки овальных геометрических предметов диаметром порядка 4…5 см. Форма сечения и внешний вид представлены на рис. 1.

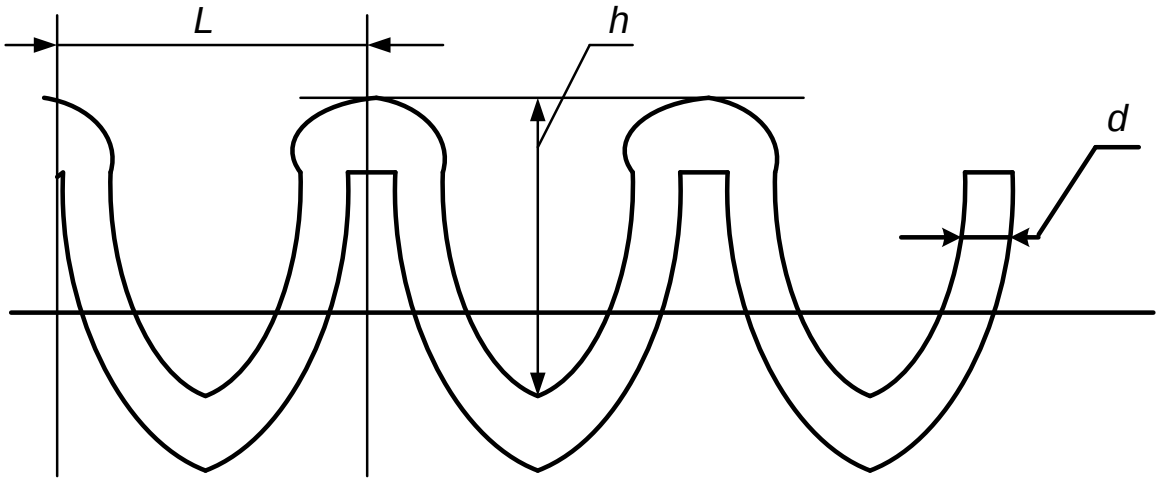


Рис. 1. Геометрические размеры пирамидообразных форм из прессованной целлюлозы, используемых для изготовления шунгитобетонных модулей с добавлением бишофита

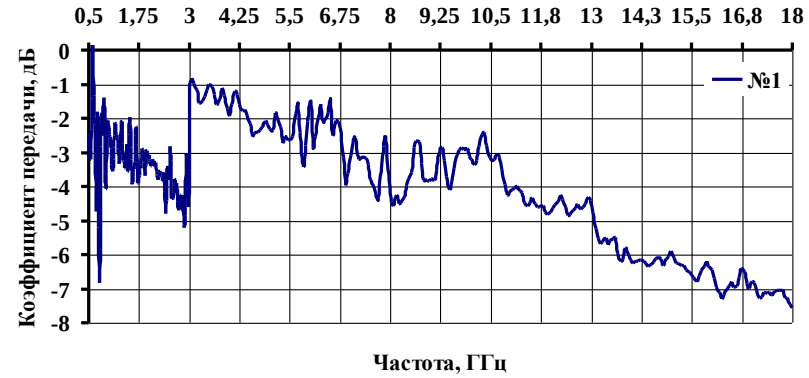
Шунгитобетон изготавливали на основе смесей порошков шунгита (размер фракций не более 0,5 мм) и портландцемента в весовом соотношении 1:4 и бишофита в соотношении 1:4 в 30%-х водных растворах хлорида кальция (CaCl2) путем заполнения таким бетоном прямоугольных деревянных опалубок размером 0,4×0,3 м. Для таких устройств дно выполнялось из пирамидообразных форм из прессованной целлюлозы.

Поверхность такого модуля из шунгитобетона выравнивали по поверхности опалубки, и ее минимальная толщина составляла 8…10 мм.

Обсуждение результатов

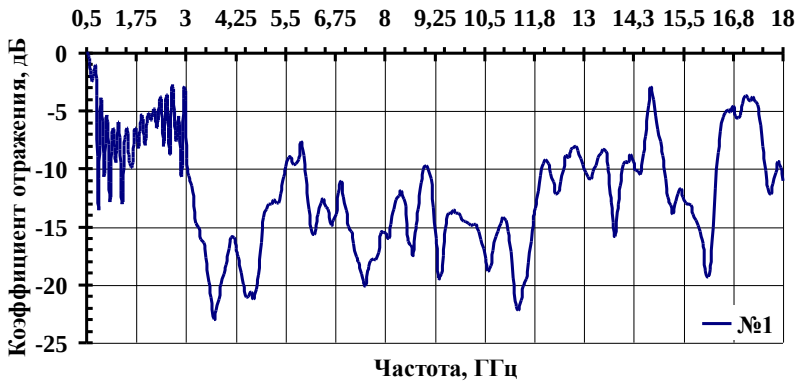
Для описанных выше образцов шунгитобетонных плит измерение характеристик ослабления и отражения проводили в диапазоне частот 0,5…18 ГГц, результаты приведены на рис. 2.

Из рис. 2 видно, что образец из шунгитобетона с добавкой бишофита в диапазоне 0,5…18 ГГц характеризируется относительно невысокой отражательной способностью (–5…–23 дБ), а значение ослабления образца в диапазоне 0,5… 18 ГГц составляет от –0,5 дБ до –8 дБ.



а

б



в

Рис. 2. Частотные зависимости экранирующих характеристик экранов ЭМИ в диапазоне частот 0,5…18 ГГц: ослабление (*а*), коэффициент отражения без металлического отражателя (*б*) и коэффициент отражения с металлическим отражателем (*в*)

Заключение

Использование пирамидообразных экранов ЭМИ с добавлением бишофита на основе углеродосодержащих материалов снижает уровень воздействия излучения на организм человека. Это обозначает, что добавка бишофита, в составе которого имеется (MgCl2 · 6H2O), оказывает существенное влияние на уменьшение коэффициента отражения в диапазоне частот от 0,5 до 18 ГГц, данные частоты являются основными в излучении персонального компьютера и могут инициировать биологические нарушения (вплоть до нарушения синтеза ДНК).

EFFECT OF PERFORMANCE BISCHOFITE PYRAMID SCHIELDS ELECTROMAGNETIC RADIATION PROTECTION OF INFORMATION AND ENVIRONMENTAL SAFETY

M.Sh. MAHMOUD, E.S. BELOUSOVA, A.M. PRUDNIK, L.M. LYNKOU

Abstract

The use of bischofite and schungite powder for creation of the electromagnetic radiation shields is proposed. Frequency dependencies of transmission and reflection coefficients of pyramid shields with addition of bischofite in the frequency range of 0,5…18 GHz are presented.

Литература

1. Защита от воздействия электромагнитных излучений. [Электронный ресурс]. Режим доступа: http://grachev.distudy.ru/Uch_kurs/sredstva/Templ_1/templ_1_6.htm.

2. *Тарченко У.А., Петровский Я.Ч., Василенко Д.А. Прудник А.М.* // Материалы XIV Международной научно-технической конференции «Современные средства связи». 29 сентября-1 октября 2009. Минск, Беларусь. С. 165.

3. *Колбун Н.В., Петров С.Н., Прудник А.М.* // Докл. БГУИР. 2009. №3. С. 79-85.

4. Bischofite Mineral Data [Электронный ресурс]. Режим доступа: http://webmineral.com/data/Bischofite.shtml.

УДК [*004.353.2:537.531*]:*537.622.6*

ЭКРАНЫ ЭЛЕКТРОМАГНИТНОГО ИЗЛУЧЕНИЯ НА ОСНОВЕ ФЕРРИМАГНИТНЫХ МАТЕРИАЛОВ

О.В. БОЙПРАВ, М.Р. НЕАМАХ, В.Б. СОКОЛОВ, Т.В. БОРБОТЬКО

Белорусский государственный университет информатики и радиоэлектроники
П. Бровки, 6, Минск, 220013, Беларусь

Поступила в редакцию 16 марта 2012

Приводятся описание и анализ результатов измерений и расчета параметров магнитных характеристик (зависимостей относительной магнитной проницаемости от величины индукции внешнего магнитного поля и температуры окружающей среды) порошкообразного шлама очистки ваграночных газов, который предложено использовать для разработки конструкций экранов электромагнитного излучения градиентного типа.

Ключевые слова: вибрационный магнитометр, индукция магнитного поля, относительная магнитная проницаемость, ферромагнетик, ферримагнетик, шлам очистки ваграночных газов, электромагнитное излучение.

Введение

Современные устройства обработки данных (УОД) базируются на микропроцессорных и микроэлектронных элементах и, в связи с этим, способны оперативно формировать и обрабатывать информационные сигналы в широком диапазоне частот. Однако в процессе своего функционирования эти устройства способны наводить друг на друга паразитные емкостные и индуктивные связи, которые могут нарушать целостность обрабатываемых данных. Снизить значения коэффициентов этих связей возможно путем обеспечения электромагнитной совместимости УОД, которое предполагает использование конструкций, экранирующих ЭМИ, в широком диапазоне частот.

Эффективность экрана ЭМИ определяется уровнем диэлектрических и магнитных потерь энергии электромагнитных волн в его материале, а также уровнем потерь на проводимость. Уровни диэлектрических и магнитных потерь в среде прямо пропорциональны значениям ее относительной диэлектрической (ε) и магнитной (μ) проницаемости. В силу этого для создания эффективного экрана ЭМИ необходимо выбирать материалы с высокими показателями ε и μ [1].

Таким образом, базовый этап разработки экранов ЭМИ сопровождается измерением и сравнением электрических параметров (электропроводности, диэлектрической проницаемости) набора предполагаемых к использованию материалов, а также исследованием и сравнительным анализом магнитных характеристик последних.

По реакции на внешнее магнитное поле и по характеру внутреннего магнитного упорядочения все вещества в природе можно разделить на пять групп: диамагнетики, парамагнетики, ферромагнетики, антиферромагнетики, ферримагнетики. Диа-, пара- и антиферромагнетики можно объединить в группу слабомагнитных веществ, относительная магнитная проницаемость которой примерно равна 1. Ферро- и ферримагнетики являются сильномагнитными материалами. Значения их относительной магнитной проницаемости зависят от величины внешнего магнитного поля (B) и лежат в пределе $10^2 \ldots 10^6$ у ферромагнетиков, $1 \ldots 10^2$ – ферримагнетиков [2, 3]. К ферромагнетикам относят железо, никель, кобальт и сплавы данных металлов. Основной недостаток ферромагнетиков заключается в их подверженности коррозии, а также низкой температурной стабильности их магнитных свойств. Данных недостатков лишены фер-

римагнетики, свойствами которых в большинстве случаев обладают различные оксидные соединения металлов, в частности, ферриты. Поэтому ферримагнетики более приемлемы, чем ферромагнетики, для изготовления конструкций, экранирующих ЭМИ. Так как перечень требований к свойствам последних является разнообразным и постоянно расширяющимся, то набор существующих ферримагнетиков следует совершенствовать, дополняя его новыми образцами. Базовый этап поиска новых ферримагнетиков включает в себя процессы выявления особенностей и исследования магнитных характеристик ранее не исследованных оксидных соединений металлов. К числу последних относится шлам очистки ваграночных газов (ШОВГ), в состав которого входят 22,66% по масс. оксида кальция, 11,37% по масс. оксида трехвалентного железа, 3,57% по масс. оксида магния, 3,38% по масс. оксида натрия, 3,25% по масс. оксида алюминия, 1,96% по масс. оксида калия, а также 24,35% по масс. оксида кремния, 2,68% по масс. оксида серы и др. [4]. ШОВГ представляет собой порошкообразные отходы, образующиеся в результате фильтрации и обработки в осевом циклоне газов, отбираемых через трубы шахтных печей в процессе переплавки в них чугуна с использованием древесного угля и кокса. Отличительной особенностью ШОВГ по сравнению с ферритами и иными оксидными соединениями металлов является его низкая стоимость.

Целью работы является исследование магнитных характеристик (зависимостей относительной магнитной проницаемости от величины внешнего магнитного поля и температуры) образцов порошкообразных соединений оксидов металлов – шлама очистки ваграночных газов (ШОВГ) – отличающихся друг от друга размером фракций.

Методика проведения эксперимента

В рамках настоящей работы были проведены измерения магнитных характеристик (зависимостей относительной магнитной проницаемости от величины внешнего магнитного поля и температуры окружающей среды) образцов порошкообразного ШОВГ, отличающихся друг от друга степенью измельчения фракций. У образцов №1 и №2 размер фракций составил 5 мкм и 20 мкм соответственно (мелкоизмельченные фракции), у образца №3 – 30 мкм (среднеизмельченные фракции).

Измерения параметров зависимостей относительной магнитной проницаемости ШОВГ от величины внешнего магнитного поля проводились при комнатной температуре и при значениях магнитной индукции, изменяющихся равномерно, с шагом 0,02 Тл, в пределах диапазона (–3 Тл…3 Тл). Измерения температурных зависимостей относительной магнитной проницаемости ШОВГ проводились в диапазоне от комнатной до гелиевой температуры при постоянном значении B, равном 0,5 Тл.

Исследование магнитных характеристик ШОВГ проводилось при помощи вибрационного метода измерений с использованием вибрационного магнитометра Cryogenic 14T VIBRATING SAMPLE MAGNETOMETER. Принцип действия прибора основан на измерении значений магнитной индукции исследуемого образца, колеблющегося в постоянном магнитном поле.

Основными узлами вибрационного магнитометра Cryogenic 14T VIBRATING SAMPLE MAGNETOMETER являются генератор механических колебаний, электронный измерительный блок, соленоид, измерительные катушки, датчик поля Холла, шток с кварцевым держателем образца. В конструкцию генератора механических колебаний входит емкостной датчик, стабилизирующий амплитуду колебаний образца. Электронный измерительный блок имеет модульную структуру. В его состав входят источник питания, генератор синусоидального сигнала с усилителем мощности для питания генератора механических колебаний, модуль управления, фазовый детектор, усилитель сигнала, поступающего с измерительных катушек, измеритель поля Холла, регистрирующий значения магнитной индукции исследуемого образца.

В процессе измерений исследуемый образец помещался в пластиковую трубку и закреплялся между фиксаторами штока. Источником магнитного поля служил соленоид. Направление колебаний образца – вертикальное, а магнитный момент образца, индуцированный внешним магнитным полем, был ориентирован горизонтально. Сигнал от измерительных катушек после фазового детектирования и усиления поступал на вход измерителя поля Холла. Генератором механических колебаний выступал электродинамический громкоговоритель,

движение образцу передавалось от него посредством штока. Амплитуда колебаний образца была постоянной и составляла 0,0344 м.

Относительная погрешность проведенных измерений составила ±1%. Источником погрешности является нестабильность частоты колебаний образца, равная 10^{-2} Гц. Возникновение данной нестабильности может быть связано с дрейфом электрических параметров схемы, питающей генератор механических колебаний.

Результаты и их обсуждение

На основании результатов измерений значений магнитной индукции образцов ШОВГ рассчитаны значения их относительной магнитной проницаемости. По результатам расчета построены зависимости относительной магнитной проницаемости ШОВГ от величины индукции внешнего магнитного поля и температуры окружающей среды.

Установлено, что относительная магнитная проницаемость ШОВГ увеличивается по мере увеличения уровня внешнего магнитного поля. Значение начальной относительной магнитной проницаемости (при $B = 0$) для образца №1 составляет 0,28, для образца №2 – 0,53, для образца №3 – 1,1, значения максимальной относительной магнитной проницаемости равны 4,04; 7,18; 41,1 соответственно. Кроме того, для образцов ШОВГ характерны явления остаточной намагниченности.

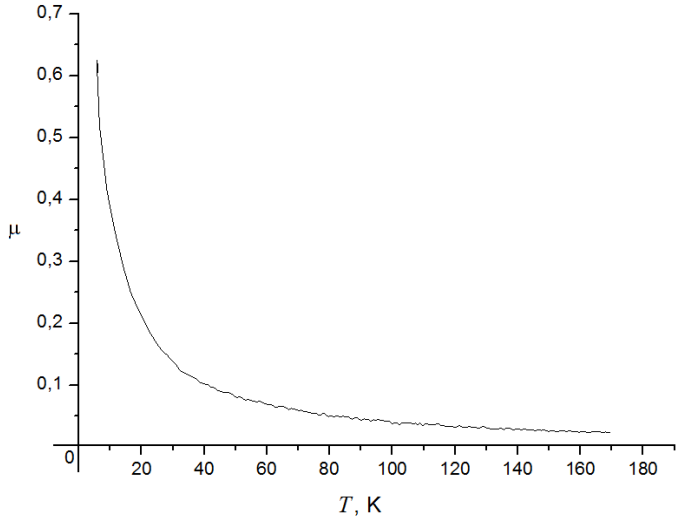


Рис. 1. Температурная зависимость относительной магнитной проницаемости образца №1

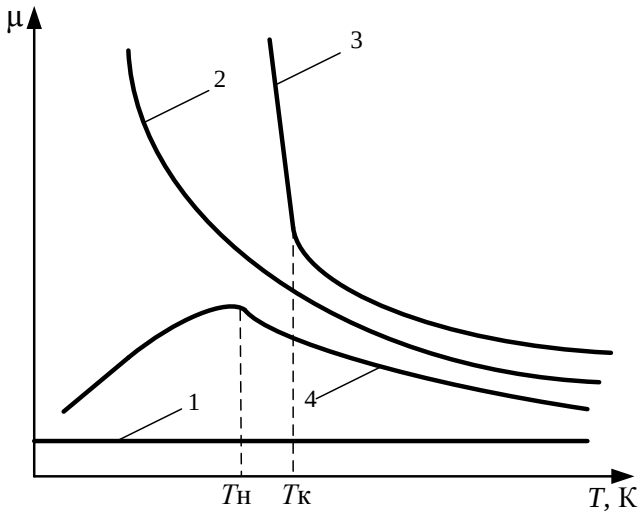


Рис. 2. Общий вид температурной зависимости относительной магнитной проницаемости диамагнетиков (1), парамагнетиков (2), ферро- и ферримагнетиков (3), антиферромагнетиков (4)

Выявлено, что относительная магнитная проницаемость ШОВГ изменяется с изменением температуры окружающей среды. Характер графика температурной зависимости относительной магнитной проницаемости ШОВГ (см. рис. 1) схож с характером аналогичного графика для ферримагнетиков (рис. 2). На рис. 2 $T_{\text{Н}}$ – точка Нееля (температура, при которой антиферромагнетик переходит в парамагнитное состояние), $T_{\text{К}}$ – точка Кюри (температура, при которой ферро- либо ферримагнетик переходит из упорядоченного магнитного состояния в неупорядоченное (парамагнитное) и тем самым утрачивает свои магнитные свойства) [5].

Для описания характера изменения магнитных свойств материала при изменении температуры окружающей среды может быть использован температурный коэффициент магнитной проницаемости (TK_{μ}) [6]

$$TK_{\mu} = \frac{\mu_2 - \mu_1}{\mu_1} \cdot \frac{1}{T_2 - T_1}, \qquad (1)$$

где μ_1 и μ_2 – значения относительной магнитной проницаемости материала при температурах T_1 и T_2 соответственно.

На основании расчета установлено, что в диапазоне отрицательных температур (169 К…6 К) среднее значение температурного коэффициента магнитной проницаемости (TK_{μ}) ШОВГ составляет 0,055 $К^{-1}$, т.е. при изменении температуры окружающей среды на 1 К значение относительной магнитной проницаемости ШОВГ изменяется на 0,055. В области гелиевых температур (27 К…6 К), значение относительной магнитной проницаемости ШОВГ начинает резко возрастать и ТКμ при этом составляет 0,2 $К^{-1}$. Подобное поведение присуще температурным зависимостям относительной магнитной проницаемости ряда ферритов [7].

Заключение

Порошкообразный ШОВГ можно отнести к новым образцам ферримагнетиков, т. к. значения его относительной магнитной проницаемости ниже 10^2, зависят от величины внешнего магнитного поля и характеризуются высокой температурной стабильностью. ШОВГ присуща способность намагничиваться в слабых магнитных полях, величина индукции которых не превышает 3 Тл.

Размер фракций ШОВГ оказывает влияние на магнитные характеристики данных порошкообразных материалов: увеличение размера фракций ШОВГ приводит к увеличению его магнитной проницаемости.

На основе порошкообразного ШОВГ можно формировать конструкции, которые будут эффективно экранировать ЭМИ. Одна из разновидностей таких конструкций может быть реализована путем засыпания порошка ШОВГ со среднеизмельченными фракциями в каналы листа сотового поликарбоната. Эти листы можно использовать для отделки внутренних стен экранируемых помещений (например, серверных комнат). В диапазоне частот 0,7...16 ГГц значения коэффициентов отражения таких конструкций составляют от –8 дБ до –16 дБ, а коэффициентов передачи – от –5 дБ до –16 дБ.

Кроме того, на основе порошкообразного ШОВГ возможно реализовать многослойные конструкции экранов ЭМИ градиентного типа, в которых магнитная проницаемость будет увеличиваться по мере перехода электромагнитной волны от одного слоя к другому. При этом в качестве первого слоя должен выступать лист сотового поликарбоната, заполненный порошком ШОВГ, обладающим наименьшим значением относительной магнитной проницаемости, т. е. с размером фракций 5 мкм, второго и третьего – порошком ШОВГ с размером фракций 20 мкм и 30 мкм соответственно. Таким образом будет улучшено согласование волновых сопротивлений начальной среды распространения электромагнитных волн и материала подобной экранирующей конструкции, что приведет к уменьшению ее коэффициента отражения и расширению рабочего диапазона частот относительно соответствующих параметров однослойных конструкций.

ELECTROMAGNETIC RADIATION SHIELDS BASED ON FERRIMAGNETIC MATERIALS

O.V. BOIPRAV, M.R. NEAMAH, V.B. SOKOLOV, T.V. BORBOTKO

Abstract

A description and analysis of the magnetic properties measurement and calculation results (dependences of the relative magnetic permeability from the external magnetic field induction and ambient temperature) of powdered sludge treatment cupola gases are shown. It's proposed to use this material for the development of electromagnetic radiation shields of the gradient type.

Литература

1. *Козловский В.В., Софиенко И.И.* // Вісник ДУІКТ. 2009. №7 (3). С. 233-245.
2. *Андреев В.М.* Материалы микроэлектронной техники. М., 1989.
3. *Гуревич А.Г.* Магнитный резонанс в ферритах и антиферромагнетиках. М., 1973.
4. Протокол испытаний № 5018 от 23.02.2011. НИИППРУП «Институт НИИСМ». Научно-исследовательская лаборатория физхимии силикатов.
5. *Великанов Д.А., Юркин Г.Ю., Патрин Г.С.* // Научное приборостроение. 2008. №3 (18). С. 86-94.
6. *Ивлев Ю.Н.* Химия радиоматериалов. М., 2003.
7. *Смит Я., Вейн Х.* Ферриты. М., 1962.

УДК 535.24

УГЛОВОЕ РАСПРЕДЕЛЕНИЕ КОЭФФИЦИЕНТОВ СПЕКТРАЛЬНОЙ ЯРКОСТИ КОМБИНИРОВАННЫХ ОБРАЗЦОВ «МЕТАЛЛ-СЕТКА»

ДЖАМАЛЬ САЛД ОМЕР[*], И.М. ЦИКМАН, Ю.В. БЕЛЯЕВ

[*]*Белорусский государственный университет информатики и радиоэлектроники*
П. Бровки, 6, Минск, 220013, Беларусь

Институт прикладных физических проблем им. А.Н. Севченко
Курчатова, 7, Минск, 220108, Беларусь

Поступила в редакцию 2 ноября 2012

Описаны результаты исследований спектральных параметров отраженного от поверхности комбинированных образцов «металл-сетка» излучения. Приведены результаты определения коэффициента спектральной яркости (КСЯ) отраженного образцами излучения для четырех характерных фазовых углов.

Ключевые слова: спектр отражения, коэффициент спектральной яркости, фазовые углы, дальность обнаружения.

Введение

Применение различных маскировочных сеток позволяет значительно снизить контраст по отношению к фонам в оптической области спектра в видимом, среднем инфракрасном и тепловом диапазонах. Однако контраст может быть усилен при использовании спектрозональной съемки [1]. При этом регистрируются изображения объектов в узких полосах интерференционных фильтров, где различие в уровне отраженного излучения объект/фон максимальны. Для минимизации подобных эффектов усиления контраста необходимо исследовать ход коэффициентов спектральной яркости излучения объектов, фонов и различных маскировочных сеток в видимом и ИК-диапазонах спектра и выбирать оптимальные варианты использования различных сеток. В условиях меняющейся освещенности (различные высоты и ориентация Солнца) при наружном наблюдении большое значение имеют угловые зависимости коэффициента спектральной яркости (КСЯ).

Методика эксперимента

КСЯ определяется отношением спектральной плотности энергетической яркости (СПЭЯ) отраженного от поверхности образца излучения к СПЭЯ диффузно-рассеивающей ламбертовской поверхности, освещенной также как и исследуемый образец. В качестве ламбертовской поверхности использовалась пластина молочного стекла МС-20.

Исследования спектральных и угловых зависимостей КСЯ образцов с использованием маскировочных сеток проводились на геометрической установке при угле падения коллимированного излучения галогенной лампы на поверхность образцов 45°. Регистрация и обработка данных измерений с получением КСЯ проводились по методике, описанной в [2]. Регистрация сигнала спектрорадиометром осуществлялась в отсчетах АЦП и записывалась в файл. Специальное программное обеспечение позволяло производить пересчет этих данных в значения КСЯ.

Относительная суммарная неопределенность измерений КСЯ составляла в области 0,38-0,9 мкм менее 5%, а в области 0,9-2,4 мкм – порядка 10%. Исследуемые образцы:

- свежесрезанный лист липы (в качестве образца фона);
- пластина металла, окрашенного в зеленый цвет;
- комбинированные образцы на основе металлической пластины с сетками.

Исследовались сетки четырех видов: на тканевой основе (размер ячеек 1,5-2 мм) с окраской двух типов; пластиковой и металлической сетками (размер ячеек 3-4 мм), окрашенными в зеленый цвет.

Результаты и их обсуждение

На рис. 1 приведены кривые КСЯ исследуемых образцов при различных фазовых углах - 45°, 75°, 90°, 100°. Фазовые углы 45° и 75° соответствуют углам наблюдения в натурных условиях вертикальной поверхности объекта при различных угловых положениях Солнца, расположенном за наблюдателем. Углы 90° и 100° соответствуют горизонтальной плоскости объектов при положении Солнца перед наблюдателем.

Из рис. 1,*а,б* видно, что КСЯ растительности плавно растет с увеличением угла наблюдения во всем рассматриваемом спектральном диапазоне. Наибольший рост значений КСЯ у растительности в видимой области спектра. В ИК-области 750-2400 нм значения КСЯ увеличиваются с увеличением фазового угла в меньшей степени. Максимальные значения КСЯ листа растительности наблюдается при фазовом угле 100°, а не при зеркальном – 90°, характерном для остальных образцов.

Особенностью металлической окрашенной пластины является резкое увеличение значений КСЯ при зеркальном угле. При таком угле объект будет резко выделяться на естественных фонах.

Для комбинированных материалов «металл-сетка» (рис. 1,*в-е*) характерно значительное снижение значений КСЯ при зеркальном угле наблюдения.

Из рисунка видно, что минимальное отличие в интегральных значениях КСЯ диапазона 0,38-2,38 мкм от листа растительности при зеркальном угле наблюдения среди образцов с сеткой наблюдается у образца – «металл+сетка» т.е. с металлической сеткой. Этот результат можно объяснить неровностью поверхности металлической сетки и переотражением и поглощением излучения между сеткой и окрашенной поверхностью металла.

Для остальных комбинированных образцов «металл-сетка» характерным является значительное увеличение значений КСЯ при зеркальном угле по сравнению со значениями при других фазовых углах, но это отличие значительно меньше, чем у металлической пластины. Для углов 45º, 75º и 100º наименьшее отличие распределения КСЯ по длинам волн от растительности наблюдается у образцов металлической пластины, покрытой маскировочными сетками на тканевой основе (рис. 1,*в-г*). Однако за счет ровной и значительной по площади поверхности плотной тканевой основы между порами сетки, при зеркальном угле данный образец значительно выделяется. Интенсивность отраженного излучения при этом возрастает в среднем в 1,5-2 раза.

Заключение

Все используемые сетки при зеркальном угле наблюдения значительно снижают величину КСЯ окрашенной поверхности металла и приближают эти значения к отражательным характеристикам растительности при регистрации в интегральном спектральном диапазоне наблюдения. Данная особенность характерна для монохромных съемочных систем при наблюдении с больших расстояний, например из космоса. Таким образом, все сетки следует использовать для уменьшения заметности гладких, с зеркальным характером отражения поверхностей объектов, что уменьшает утечку информации по оптическим каналам приборов видеонаблюдения. При проведении спектрозональной съемки в нескольких узких спектральных диапазонах важна не только интегральная величина яркости, но и характерный для природных фонов ход спектральной кривой КСЯ. Но и в этом случае использование данных сетчатых материалов, особенно сеток на тканевой основе с камуфляжной окраской, значительно уменьшают заметность объектов на природных фонах для рассматриваемых фазовых углов и, соответственно позволяет во многих случаях значительно сократить дальность обнаружения скрываемых объектов.

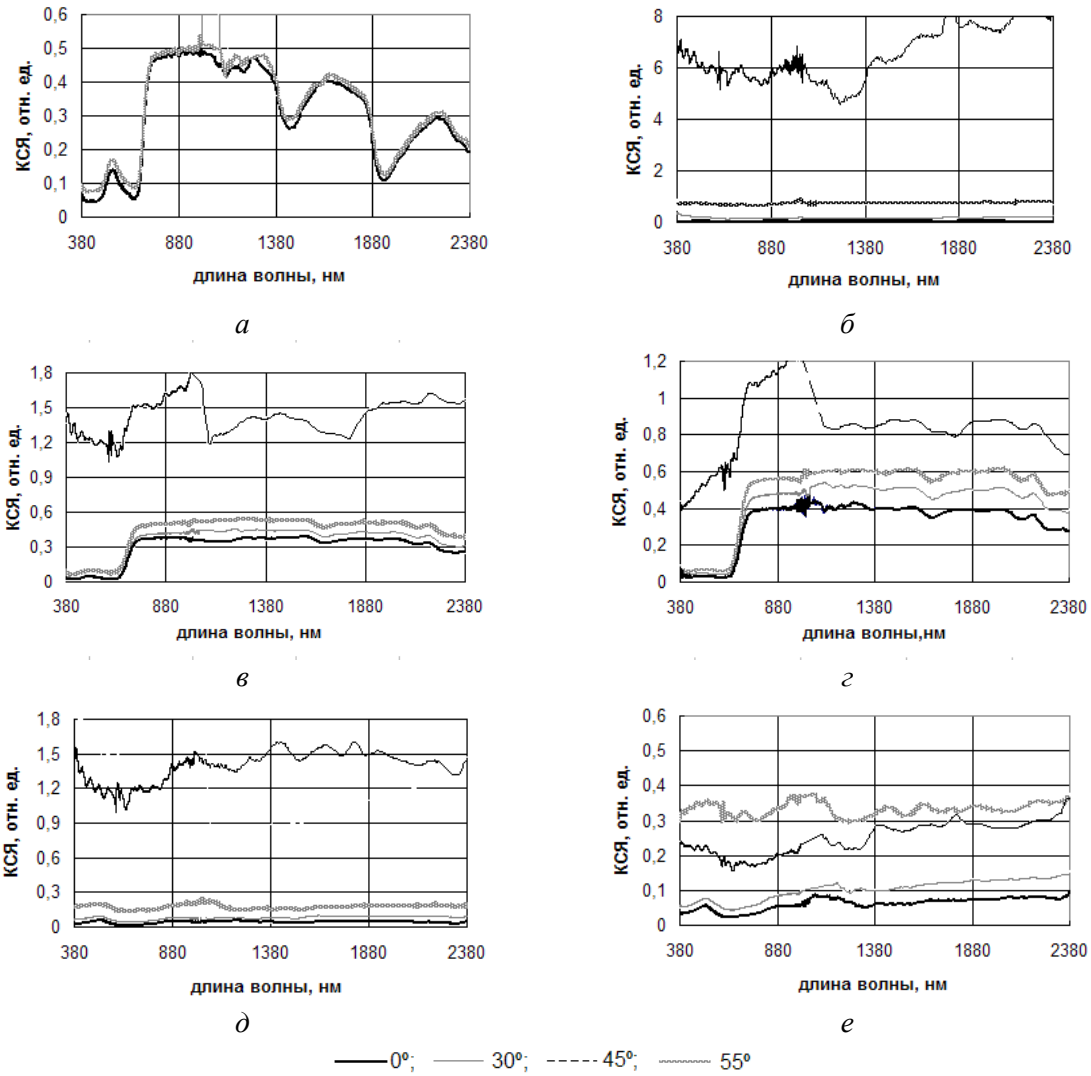


Рис. 1. Распределение КСЯ при углах наблюдения 0º, 30º, 45º, 55º:
а – лист растительности; *б* – окрашенный металл;
в – металл + тканевая сетка 1; *г* – металл + тканевая сетка 2;
д – металл + пластиковая сетка; *е* – металл + металлическая сетка

ANGULAR DISTRIBUTIONS OF THE SPECTRAL BRIGHTNESS OF COMBINED SAMPLE METAL-NET

JAMAL SAAD OMER, I.M. TSYKMAN, Y.V. BELYAEV

Abstract

The studies results of the spectral parameters of the reflected radiation from the composite «metal-net» samples surface are shown. The results of the determination of the spectral brightness coefficient radiation reflected by the sample on four characteristic phase angles are shown.

Литература

1. *Беляев Ю.В., Катковский Л.В., Курикина Т.М. и др.* // Журн. прикл. спектр. 2001. Т. 68, №2. С. 258-263.
2. *Беляев Ю.В., Омер Дж. Саад, Цикман И.М.* // Докл. БГУИР. 2011. №1. С.75-79.

УДК 004.056:654

МЕТОДИКА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ПРЕДПРИЯТИИ ОТРАСЛИ СВЯЗИ

В.А. БОЙПРАВ, О.В. БОЙПРАВ, Л.М. ЛЫНЬКОВ

Белорусский государственный университет информатики и радиоэлектроники
П. Бровки, 6, Минск, 220013, Беларусь

Поступила в редакцию 10 апреля 2012

Проведен анализ мероприятий, подлежащих реализации непосредственно перед проведением процедуры составления или дополнения стратегической и тактической политик информационной безопасности предприятия отрасли связи, включающего в себя несколько филиалов и структурных подразделений.

Ключевые слова: аудит системы информационной безопасности, информационная безопасность, отрасль связи, стратегическая политика информационной безопасности, тактическая политика информационной безопасности.

Введение

Согласно Закону Республики Беларусь от 19 июля 2005 г. №45-З, измененному и дополненному 22 декабря 2011 г., деятельность в области электросвязи в Республике Беларусь должна осуществляться на основе принципов доступности услуг электросвязи общего пользования, приоритета прав и законных интересов пользователей услуг электросвязи, равенства прав на получение услуг электросвязи, тайны телефонных и иных сообщений, устойчивости и управляемости сетей электросвязи, единства обязательных для соблюдения технических требований в области электросвязи [1]. Реализация перечисленных принципов должна сопровождаться реализацией мероприятий по обеспечению информационной безопасности (ИБ) организации отрасли связи. Причем совокупность данных мероприятий следует своевременно отображать в политике информационной безопасности (ПИБ). Ее объем и структура определяются размером организации и количеством ее персонала.

В Республике Беларусь крупнейшей организацией в отрасли связи является республиканское унитарное предприятие (РУП) «Белтелеком», предоставляющее населению и организациям страны услуги телеграфа, телефонии, сети Интернет, проводного вещания, хостинга и цифрового интерактивного телевидения. На сегодняшний день количество абонентов РУП «Белтелеком» составляет более 4,5 миллионов физических и юридических лиц. При этом стратегическая цель РУП «Белтелеком» состоит в своевременности удовлетворения спроса на перечисленные услуги.

РУП «Белтелеком» включает в себя 10 филиалов: Брестский филиал, Витебский филиал, Гомельский филиал, Гродненский филиал, Могилевский филиал, Минский филиал, филиал «Минская городская телефонная сеть», филиал «Междугородная связь», филиал «Минская телеграфно-телефонная станция», филиал «Подсобное сельское хозяйство», а также 2 структурных подразделения в составе аппарата управления («Международный центр коммутации», «Информационно-расчетный центр»). Поэтому для РУП «Белтелеком», наряду с дополнением стратегической (общей) ПИБ, следует составлять и/или дополнять тактические (частные) ПИБ, описывающие совокупность мер, которые следует предпринимать для обеспечения ИБ филиалов и структурных подразделений. Перед дополнением стратегической ПИБ РУП «Белтелеком» и дополнением/составлением тактических ПИБ его филиалов (структурных подразделений), следует провести аудит его системы ИБ. На основании результатов аудита определяется

базовая система актуальных мер по обеспечению ИБ организации. Данные меры позволяют уменьшить риски ИБ до приемлемой величины.

Последовательность действий при проведении аудита системы информационной безопасности предприятия

С целью ускорения процедуры проведения аудита системы ИБ РУП «Белтелеком» следует назначить 12 аудиторских групп и закрепить за каждой из них определенный филиал (структурное подразделение).

На первом этапе аудита системы ИБ РУП «Белтелеком» руководителем аудиторских групп должно проводиться анкетирование генерального директора организации и директоров ее филиалов (структурных подразделений). Перечень основных вопросов для анкет представлен в таблице [2].

Перечень основных вопросов для анкетирования генерального директора организации и директоров ее филиалов (структурных подразделений)

Кому адресован вопрос	Формулировка вопроса
Генеральный директор организации	Проведена ли классификация информации, обрабатываемой в рамках информационной системы Вашей организации?
	Как давно обновлялась стратегическая ПИБ Вашей организации?
	Создан ли в РУП «Белтелеком» форум для обсуждения стратегической и тактической ПИБ и информационных рисков?
	Проводятся ли среди руководства РУП «Белтелеком» регулярные совещания по вопросам координации действий по поддержанию режима безопасности? Если да, то как часто?
	Проведено ли разграничение доступа к информационной системе Вашей организации?
Директора филиалов (структурных подразделений) организации	Ознакомлены ли Вы со стратегической ПИБ РУП «Белтелеком»?
	Есть ли у Вашего филиала (структурного подразделения) тактическая ПИБ?
	Если есть, то как давно она обновлялась?
	Есть ли в Вашем филиале (структурном подразделении) сотрудник, отвечающий за принятие мер по обеспечению ИБ и контроль выполнения стратегической и тактической (при ее наличии) ПИБ РУП «Белтелеком»?
	Проводите ли Вы с руководителями отделов своих филиалов (структурных подразделений) совещания по вопросам ИБ? Если да, то как часто?
	Проведена ли классификация информации, обрабатываемой в рамках информационной системы Вашего филиала (структурного подразделения)?
Генеральный директор и директора филиалов (структурных подразделений) организации	Доводите ли Вы до сведения нанимаемых сотрудников положения стратегической ПИБ РУП «Белтелеком» и тактических ПИБ его филиалов (структурных подразделений)?
	Когда в последний раз руководители отделов Вашей организации, работающих с информационной системой, проходили обучение по вопросам ИБ?
	Когда в последний раз в Вашей организации проводился аудит системы ИБ?
	Были ли ознакомлены руководители отделов Вашей организации, работающих с информационной системой, с результатами проведенного аудита?
	Проходила ли система защиты информационной системы Вашей организации аттестацию в соответствии с «Положением о порядке аттестации систем защиты информации» утвержденным Постановлением Совета Министров Республики Беларусь от 26.05.2009г. № 675? [3]

В рамках второго этапа экспертами аудиторских групп должна осуществляться проверка защищенности корпоративной сети каждого из филиалов: установление частоты обновления антивирусного программного обеспечения и наличия (выполнения) разделов ПИБ, касающихся политики управления компьютерными паролями и разграничения доступа к данным персональных компьютеров. В рамках второго этапа следует провести анкетирование с системными администраторами корпоративной сети организации, а также корпоративных сетей ее филиалов (структурных подразделений). Среди основных вопросов для анкет системных администраторов должны быть следующие. Установлено ли на персональных компьютерах сотрудников Вашего филиала (структурного подразделения) антивирусное программное обеспечение? Проверка жестких и съемных дисков персональных компьютеров сотрудников Вашего филиала на наличие вирусов производится вручную, либо с использованием сканеров? Произведена ли настройка источника и периодичности обновления вирусных сигнатур антивирусного программного обеспечения? Знают ли сотрудники Вашего филиала последовательность действий при обнаружении вируса антивирусным программным обеспечением? [4]

На третьем этапе следует проводить проверку наличия и исправности систем контроля и управления доступом (дверей, замков, оконных решеток и т.д.), систем охранной и противопожарной сигнализации в помещениях, где располагается оборудование, диагностику их климатических условий (температура и влажность воздуха, наличие вентиляционной системы и системы кондиционирования) [5].

Результаты аудита ИБ филиалов должны быть сведены в итоговые отчеты ответственными по каждой из аудиторских групп. Директора филиалов (структурных подразделений) должны быть ознакомлены с положениями этих отчетов перед проведением собрания по закрытию аудита.

На основании данных итоговых отчетов руководитель аудиторских групп готовит общий итоговый отчет и доносит его положения на собрании по закрытию аудита до генерального директора организации и директоров ее филиалов (структурных подразделений).

Обработка результатов аудита системы информационной безопасности предприятия

На основании положений общего итогового отчета об аудите системы ИБ РУП «Белтелеком» осуществляется дополнение его стратегической ПИБ. В состав рабочей группы по дополнению стратегической ПИБ РУП «Белтелеком» следует включать генерального директора организации, заместителя генерального директора по техническим вопросам, заместителя генерального директора по персоналу, директоров филиалов (структурных подразделений), начальника службы безопасности, начальника юридического отдела, технического писателя, а также независимого эксперта по разработке ПИБ (руководителя аудиторских групп, проводивших аудит ИБ организации).

На основании положений итоговых отчетов об аудите системы ИБ филиалов (структурных подразделений) РУП «Белтелеком», а также положений дополненной стратегической ПИБ осуществляется дополнение его тактических ПИБ. В состав рабочей группы по дополнению тактических ПИБ РУП «Белтелеком» следует включать директоров филиалов (структурных подразделений), главных инженеров, начальника службы безопасности, юристов, технических писателей, а также независимых экспертов по разработке ПИБ (ответственных по аудиторским группам, проводившим аудит ИБ филиалов (структурных подразделений)).

Положения стратегической и тактической ПИБ РУП «Белтелеком» для его сотрудников должны носить не рекомендательный, а обязательный характер. Ответственность за нарушение положений ПИБ должна быть четко определена и возложена на директоров филиалов (структурных подразделений) РУП «Белтелеком».

Во всех филиалах (структурных подразделениях) должен быть назначен сотрудник, отвечающий за принятие мер по обеспечению ИБ и контроль выполнения положений стратегической и тактической ПИБ (в случае, если он не был назначен ранее). Кроме того, необходимо назначить сотрудника, который будет вести контроль выполнения всеми филиалами (структурными подразделениями) РУП «Белтелеком» положений стратегической ПИБ путем регулярного проведения проверок.

За нарушение положений ПИБ должны быть предусмотрены конкретные дисциплинарные, административные взыскания и материальная ответственность, возлагаемые как на работника, не соблюдающего положения ПИБ, так и на сотрудника филиала (структурного подразделения), осуществляющего контроль выполнения ПИБ, а также директора данного филиала (структурного подразделения).

С изменениями и дополнениями стратегической и тактической ПИБ РУП «Белтелеком», а также с перечнем мер, предпринимаемых в случае невыполнения ее положений, должен быть под роспись ознакомлен каждый сотрудник организации, имеющий доступ к информационной системе.

При этом при внесении новых положений в ПИБ стоит учитывать то, что они должны однозначно истолковываться сотрудниками, для которых предназначены. Кроме того, соблюдение положений ПИБ не должно в значительной степени оказывать влияния на темпы выполнения сотрудниками своих прямых обязанностей, прописанных в должностных инструкциях.

В организации должны быть предусмотрены меры по реагированию на нарушение положений ПИБ, в частности – оповещение об инциденте сотрудников организации, процедуры восстановления утерянных либо поврежденных данных, механизмы сбора доказательств нарушения положений стратегической либо тактической ПИБ, проведение расследования, выявление нарушителей и привлечение нарушителей к ответственности.

Заключение

Регулярно проводимый аудит системы безопасности каждого из филиалов (структурных подразделений) РУП «Белтелеком» позволит поддерживать актуальность положений его стратегической и тактической ПИБ, а также более рационально управлять денежными средствами, направляя их не на восстановление работоспособности телекоммуникационного оборудования и целостности данных, обрабатываемых в рамках информационной системы, а на расширение пакетов и улучшение качества услуг, предоставляемых населению и организациям страны, модернизацию телекоммуникационного оборудования, повышение профессиональной грамотности сотрудников.

METHODS FOR MAINTENANCE INFORMATION SECURITY IN THE TELECOMMUNICATION SECTOR ORGANIZATION

V.A. BOIPRAV, O.V. BOIPRAV, L.M. LYNKOU

Abstract

The analysis of measures to be implemented before the procedure of preparation or add strategic and tactical information security policies enterprise communications industry, including a number of subsidiaries and business units, is conducted.

Литература

1. Закон Республики Беларусь от 19 июля 2005 г. №45-З «Об электросвязи».
2. ISO 27001-2005. Системы управления информационной безопасностью.
3. Система защиты информации. [Электронный ресурс]. Режим доступа: http://itsec.by/audit-informatsionnoy-bezopasnosti-primer/.
4. Аудит информационной безопасности. [Электронный ресурс]. Режим доступа: http://itsec.by/predvaritelnaya-obshhaya-ocenka-sistemy-zashhity-informacii-gosudarstvennoj-informacionnoj-sistemy-anketa-voprosnik-chast-2/.
5. *Бойправ В.А., Бойправ О.В., Лыньков Л.М.* // Матер. XVII Межд. науч.-техн. конф. «Современные средства связи». Минск, 2012. С. 249.

СВЕДЕНИЯ ОБ АВТОРАХ

1.	Аль-Хаснави Удай Махмуд	- магистрант кафедры сетей и устройств телекоммуникаций БГУИР
2.	Аль-Шамари Карар Талал Хамза	- магистрант кафедры сетей и устройств телекоммуникаций БГУИР
3.	Беляев Юрий Владимирович	- к.т.н., заведующий лабораторией оптико-физических измерений НИИПФП им. А.Н. Севченко БГУ
4.	Белоусова Елена Сергеевна	- аспирант кафедры защиты информации БГУИР
5.	Богрецов Владимир Андреевич	- аспирант кафедры алгебры и защиты информации БГУ
6.	Бойправ Владимир Андреевич	- магистрант кафедры защиты информации БГУИР
7.	Бойправ Ольга Владимировна	- аспирант кафедры защиты информации БГУИР
8.	Борботько Тимофей Валентинович	- д.т.н., доцент кафедры защиты информации БГУИР
9.	Борискевич Анатолий Анатольевич	- к.т.н., доцент кафедры сетей и устройств телекоммуникаций БГУИР
10.	Варец Любава Ярославовна	- магистрант кафедры сетей и устройств телекоммуникаций БГУИР
11.	Волков Кирилл Аркадьевич	- аспирант кафедры сетей и устройств телекоммуникаций БГУИР
12.	Джамаль Саад Омер	- аспирант кафедры защиты информации БГУИР
13.	Киевец Наталья Григорьевна	- аспирант кафедры защиты информации БГУИР
14.	Ким Антон Дмитриевич	- магистрант кафедры сетей и устройств телекоммуникаций БГУИР
15.	Конопелько Валерий Константинович	- д.т.н., профессор, зав. кафедрой сетей и устройств телекоммуникаций БГУИР
16.	Корзун Александр Иванович	- к.т.н., доцент кафедры защиты информации БГУИР
17.	Королев Алексей Иванович	- к.т.н., доцент кафедры сетей и устройств телекоммуникаций БГУИР
18.	Липницкий Валерий Антонович	- д.т.н., профессор, зав. кафедрой высшей математики и физики ВА

СВЕДЕНИЯ ОБ АВТОРАХ

19.	Лыньков Леонид Михайлович	- д.т.н., профессор, зав. кафедрой защиты информации БГУИР
20.	Макейчик Екатерина Геннадьевна	- аспирант кафедры сетей и устройств телекоммуникаций БГУИР
21.	Махмуд Мохаммед Шакер	- аспирант кафедры защиты информации БГУИР
22.	Митюхин Анатолий Иванович	- к.т.н., доцент кафедры физико-математических дисциплин ИИТ БГУИР
23.	Неамах Мустафа Рахим	- аспирант кафедры защиты информации БГУИР
24.	Охрименко Алексей Алексеевич	- аспирант кафедры защиты информации БГУИР
25.	Подлуцкий Алексей Александрович	- аспирант кафедры сетей и устройств телекоммуникаций БГУИР
26.	Прудник Александр Михайлович	- к.т.н., доцент кафедры защиты информации БГУИР
27.	Руис Эченагусиа Луис Альфонсо	- аспирант кафедры сетей и устройств телекоммуникаций БГУИР
28.	Салас Валор Нестор Альфредо	- аспирант кафедры сетей и устройств телекоммуникаций БГУИР
29.	Саломатин Сергей Борисович	- к.т.н., доцент кафедры сетей и устройств телекоммуникаций БГУИР
30.	Селиванова Юлия Александровна	- магистрант кафедры сетей и устройств телекоммуникаций БГУИР
31.	Соколов Владимир Борисович	- ассистент кафедры электроники БГУИР
32.	Хоанг Нгок Зыонг	- аспирант кафедры сетей и устройств телекоммуникаций БГУИР
33.	Цветков Виктор Юрьевич	- к.т.н., доцент кафедры сетей и устройств телекоммуникаций БГУИР
34.	Цикман Ирина Михайловна	- младший научный сотрудник лаборатории оптико-физических измерений НИИПФП им. А.Н. Севченко БГУ
35.	Юревич Андрей Александрович	- аспирант кафедры сетей и устройств телекоммуникаций БГУИР

ISBN 978-985-488-834-7