МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ Н.Г. ЧЕРНЫШЕВСКОГО»

Кафедра теоретических основ компьютерной безопасности и криптографии

Размножение ошибок в мажоритарных декодерах

АВТОРЕФЕРАТ
дипломной работы

студентки 6 курса 631 группы
специальности 10.05.01 Компьютерная безопасность
факультета компьютерных наук и информационных технологий
Юдиной Татьяны Игоревны

Научный руководитель
доцент, к.ф.-м.н., доцент _____ А.Н.Гамова
22.01.2022 г.

Заведующий кафедрой
д. ф.-м. н., доцент _____ М. Б. Абросимов
22.01.2022 г.

Саратов 2022

ВВЕДЕНИЕ

Мы окружены информацией, постоянно получаем и передаем ее другим людям по всему миру. Но всякий раз, когда сообщение отправляется по телефону, через Интернет или через спутники, вращающиеся вокруг Земли, существует вероятность возникновения ошибок. Фоновый шум, технические неисправности, даже космические лучи способны повредить сообщение и важная информация может быть потеряна или сильно искажена. Однако существуют способы кодирования сообщения, которые позволяют автоматически обнаруживать и исправлять ошибки. Данное направление получило название — помехоустойчивое кодирование. Оно нашло своё применение не только в процессах передачи информации, но и в хранении данных.

Целью данной работы является рассмотрение и изучение помехоустойчивых кодов, основанных на мажоритарной логике, и практическая реализация на примере кода Рида-Маллера.

Коды Рида-Маллера являются одними из самых старых кодов, исправляющих ошибки, но актуальными до сих пор. Они стали более распространенными по мере развития телекоммуникаций и использования кодов, способных к самокоррекции. Коды Рида-Маллера были изобретены в 1954 году Д. Э. Маллером и И. С. Ридом. В 1972 году код Рида-Маллера вышел на новый уровень и был использован аппаратом Mariner 9 для передачи черно-белых фотографий Марса [1].

Для достижения цели, поставленной в данной дипломной работе, была необходимость решить следующие задачи:

- изучить методы помехоустойчивого кодирования;
- рассмотреть принципы мажоритарно декодируемых кодов, как блочных, так и сверточных;
- исследовать эффект размножения ошибок;
- выбрать алгоритм для реализации помехоустойчивого кода;

- создать программу, реализующую кодирование и декодирование выбранным методом для разных входных данных;
- проанализировать работу алгоритма.

Дипломная работа состоит из введения, 4 разделов, заключения, списка использованных источников и 1 приложения. Общий объем работы – 43 страницы, из них 33 страницы – основное содержание, включая 21 рисунок и 1 таблицу, список использованных источников из 21 наименований.

КРАТКОЕ СОДЕРЖАНИЕ

Первый раздел «Помехоустойчивые коды и область их применения» состоит из двух подразделов, первый из которых знакомит нас с методами, способными обнаружить ошибки при передаче информации. К их числу можно отнести проверку, включающую хэш-функцию. Во втором подразделе рассказано о подходах, которые применяются в случае обнаружения ошибки для её исправления. Выделяют два основных метода:

1. автоматический запрос на повторение, который часто используется в Интернете;
2. коды, исправляющие ошибки, которым посвящена эта работа.

Наряду с разработкой кода идет разработка эффективного декодера, который используется для быстрого и надежного исправления поврежденных сообщений. Изначально ведущими направлениями были – создание методов декодирования на базе алгебры конечных полей. Затем интерес специалистов привлекли мажоритарные методы, которые образуют класс линейных кодов, как сверточных, так и блоковых, имеющих ортогональные проверки. Именно эти методы используются для исправления ошибок.

Так что во втором разделе рассматривается механизм мажоритарного декодирования сверточных кодов. В свою очередь этот раздел включает в себя четыре подраздела. Первый знакомит нас с понятием сверточного кода и его основными свойствами, такими как: непрерывность, наличие памяти, хорошие характеристики и рекуррентность.

Второй подраздел описывает схему сверточного кодера в общем виде, представленной на рисунке 4. В сверточном кодировании вход и выход кодера представляют собой непрерывные потоки цифр. Кодер выводит n выходных цифр для каждого k введенных цифр, и код описывается как «код скорости k/n». К основным элементам кодера будут относиться:

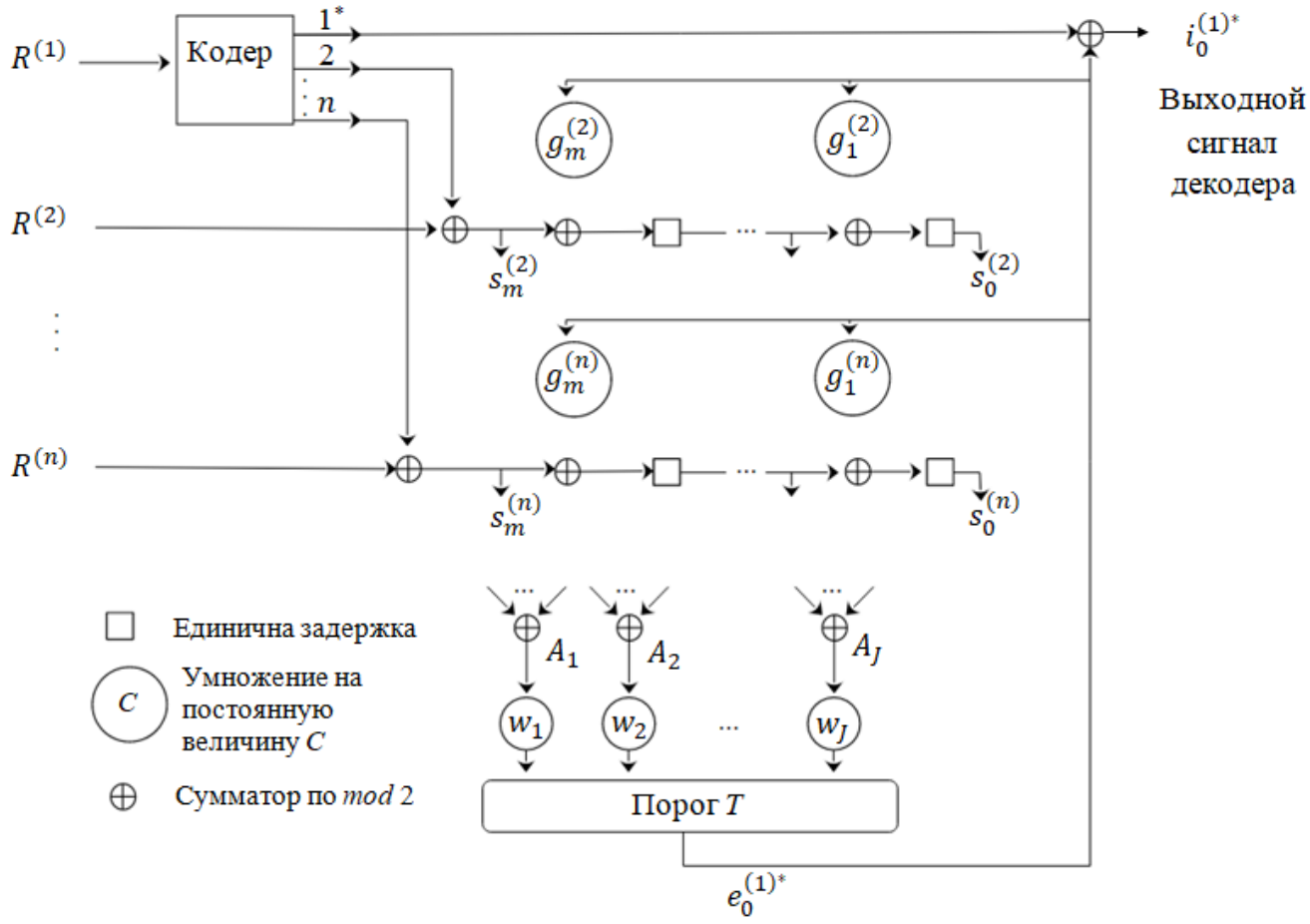
1. регистр сдвига;
2. сумматор;
3. коммутатор.

Рисунок 4 – Сверточный кодер в общем виде

где входная последовательность $I = \{i_j\}$, при $j = 1, \dots, k;$

а выходная последовательность $T = \{t_j\}$, при $j = 1, \dots, n;$

Третий подраздел второго раздела есть описание декодера сверточного кода, представленного на рисунке 6. Данная схема показывает метод описанный Джеймсом Месси в одной из своих книг.



6 – Схема порогового декодера сверточного кода скорости $1/n$

Для варианта сверточного кода со скоростью $R = k/n$ один пороговый элемент заменяется на k аналогичных логических элементов.

В строении декодера из рассмотренной схемы присутствует модель обратных связей, которая хоть и улучшает эффективность работы, но значительно увеличивает эффект размножения ошибок, речь о котором идёт в заключительном подразделе этого раздела. Были предприняты попытки исправления группирования ошибок с помощью методов повторного декодирования принятых сообщений, но результата это не дало. На практике часто применяют блоковые коды, которые не подвержены данному эффекту. Примером такого кода является код Рида-Маллера. Ему посвящен третий раздел работы, который также включает в себя несколько подпунктов.

Первый подпункт описывает основные определении, термины и операции, которые используются в кодах Рида-Маллера $R(r, m)$. Параметры, которые однозначно могут описать данный метод это порядок r и длина $n = 2^m$.

Второй подпункт объясняет достаточно простой принцип кодирования способом Рида-Маллера и описывает построение корректирующей матрицы, которая будет состоять из $k = 1 + (\mathrm{C}_m^1) + (\mathrm{C}_\mathrm{m}^2) + \ldots + (\mathrm{C}_\mathrm{m}^\mathrm{r})$ строк.

Пусть $m = (m_1, m_2, \ldots m_k)$ – блок сообщения M, тогда закодированное сообщение будет иметь следующий вид:

$$M_c = \sum_{i=1}^{k} m_i R_i$$

где R_i – строка матрицы кодирования $R(r,\ m)$.

И третий подпункт описывает алгоритм декодирования. Это является более сложной задачей, чем кодирование. Используемый метод декодирования проверяет каждую строку матрицы кодирования и с помощью мажоритарной логики определяет, была ли эта строка использована при формировании кодированного сообщения. Таким образом, можно определить, каким было закодированное сообщение без ошибок и каким было исходное сообщение. Этот метод декодирования представлен следующим алгоритмом:

Примените шаги 1 и 2 ниже к каждой строке матрицы, начиная снизу и работая вверх.

Шаг 1. Необходимо выбрать строку в порождающей матрице $R(r,m)$. Найти 2^{m-r} характеристических вектора для этой строки, а затем взять скалярное произведение каждой из этих строк с кодированным сообщением.

Шаг 2. Далее взять большинство значений скалярных произведений и присвоить это значение коэффициенту ряда.

Шаг 3. После выполнения шагов 1 и 2 для каждой строки, кроме верхней, снизу вверх матрицы, необходимо умножить каждый коэффициент на соответствующий ряд и сложить полученные векторы, чтобы сформировать M_y. Далее добавить результат к полученному закодированному сообщению. Если в полученном векторе больше единиц, чем нулей, то коэффициент верхней строки равен 1, в противном случае - 0. Добавление верхней строки, умноженной на свой коэффициент, к M_y дает исходное закодированное сообщение. Таким образом, можно определить ошибки. Вектор, образованный последовательностью коэффициентов, начиная с верхней строки матрицы кодирования и заканчивая нижней строкой, является исходным сообщением.

Количество ошибок, которые сможет исправить такой алгоритм – $\frac{d-1}{2}$, где $d = 2^{m-r} -$ кодовое расстояние.

В четвертом разделе приводится описание реализованной в ходе выполнения дипломной работы программы. Она осуществляет процесс кодирования и декодирования методом Рида-Маллера, описание которого приводится ранее. Программа работает в трех режимах: вектор, текст и изображение. Для входных данных имитируется процесс передачи данных по зашумленному каналу, где имеется возможность вручную задать параметр вероятности возникновения помех.

Обработка вектора – является основополагающим режимом работы, в то время как текст и изображение дают более наглядный результат.

Еще четвертый раздел включает в себя скриншоты процесса работы программы, на которых приводятся примеры функционирования алгоритма с различными входными параметрами. Опираясь на полученные данные можно сделать вывод, что код первого порядка будет самым оптимальным в соотношении избыточности и количества ошибок, которые может исправить. И при увеличении зашумленности канала можно увеличивать параметр m для безошибочной передачи данных.

Листинг программы приведен в приложении А.

ЗАКЛЮЧЕНИЕ

Кодирование и декодирование сообщений происходит повсюду в результате работы современных технологий для передачи данных. Ошибки – довольно частое явление при обмене информацией по тем или иным каннам связи, учитывая количество используемых нами данных. Это означает, что существует необходимость в коррекции этих ошибок. Фактически, каждая передача данных включает в себя некоторый код обнаружения/исправления ошибок для защиты передаваемой информации.

В данной работе были представлены примеры некоторых видов кодов, исправляющих ошибки, в частности подробно разобран код Рида-Маллера.

В первом разделе детально были рассмотрены методы обнаруживающие и исправляющие ошибки и область их применения в современном мире.

Второй раздел был посвящен мажоритарному декодированию сверточных кодов. Были даны центральные определения, рассмотрены общие схемы кодирования и декодирования этим способом, а там же были сделаны выводы по одному из главных недостатков такого подхода, а именно – об эффекте размножения ошибок.

В следующем разделе речь шла уже о мажоритарном методе декодирования для блочных кодов на примере одного из самых популярных алгоритмов – кода Рида-Маллера. Были подробно описаны принципы кодирования и декодирования выбранным методом.

Работа описанного алгоритма для разных параметров кода была разобрана в заключительном разделе.

В начале работы говорилось, что код Рида-Маллера $R(1,5)$ использовался NASA для передачи снимков с Марса, теперь можем указать причину такого выбора. Она заключается, прежде всего, в его способности исправлять многочисленные ошибки, возникающие при передаче данных. Например, если для сообщения длины $n = 32$ в $R(1,5)$ возникает не более 7 ошибок, то алгоритм декодирования Рида-Маллера может их исправить. Это означает, что $R(1,5)$ выдерживает достаточно шумные каналы, и поэтому он хорошо

подходил для космического корабля Mariner 9 для передачи изображений с Марса.

Таким образом все поставленные задачи были полностью решены и, следовательно, цель дипломной работы была достигнута.