МИНОБРНАУКИ РОССИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО
ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ

"САНКТ-ПЕТЕРБУРГСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ ПЕТРА ВЕЛИКОГО"

Институт компьютерных наук и технологий

Направление **02.03.01** : Математика и компьютерные науки

ОТЧЕТ О ВЫПОЛНЕНИИ ПРАКТИЧЕСКОГО ЗАДАНИЯ 3

Исполнитель: _____ Яшнова Дарья Михайловна
группа 5130201/20002

Руководитель: _____ Моторин Дмитрий Евгеньевич

«___»_____ 2024г

Санкт-Петербург, 2024

Введение

В данном отчете представлен результат выполнения практического задания №3. В рамках задания требовалось создать проект в stack, закодировать текст в изображение, а затем осуществить декодирование текста из изображения.

В ходе выполнения практической работы реализуется проект на языке Haskell. В проекте была разработана программа, которая кодирует текст в изображение и декодирует текст из изображения с помощью шифра Цезаря. Программа принимает на вход изображение, текстовый файл и сдвиг для шифра. Для декодирования требуется закодированное изображение.

Проект был реализован в интегрированной среде разработки Visual Studio Code версии 1.95.2 на языке Haskell версии 9.4.8. В проекте используются расширения основных программ .hs, а также структура проекта .cabal и .yaml.

Содержание

1 Постановка задачи

Нужно реализовать кодирование текста шифром Цезаря в картинку, а далее декодировать текст из картинки. Кодирование осуществляется следующим образом:

- Текст кодируется шифром Цезаря с заданным сдвигом.
- В каждом байте изображения заменяется последний бит, последние 2 бита,..., последние 8 бит на биты из закодированного текста.

Для декодирования требуется извлечь закодированные биты из картинки и декодировать в текст, используя информацию о сдвиге.

Программа принимает 24-разрядную картинку формата bmp. Закодированный текст должен полностью помещаться в картинку и быть не менее 1000 символов. В работе должен быть использован текст биографии ученого Лебедева А.С. и его портрет в качестве картинки.

Все чистые функции должны быть вынесены в Lib.hs.

2 Описание реализации

2.1 Шифр Цезаря

Шифр Цезаря, также известный как шифр сдвига или код Цезаря — разновидность шифра подстановки, в котором каждый символ в открытом тексте заменяется символом, находящимся на некотором постоянном числе позиций левее или правее него в алфавите (рис.3).

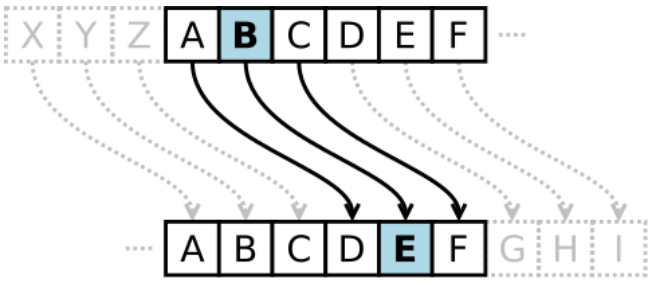

Рис. 1: Пример шифра Цезаря для сдвига 3 для латинского алфавита

Если сопоставить каждому символу алфавита его порядковый номер (нумеруя с 0), то шифрование и дешифрование можно выразить формулами модульной арифметики:

$$y = (x + k)\ mod\ n,$$

$$x = (y - k)\ mod\ n,$$

где x — символ открытого текста,
y — символ шифрованного текста,
n — мощность алфавита, k — ключ. В данной работе используется биография на русском языке. Для кодирования русских символов латинский алфавит вынесен в отдельный список.

2.2 Материалы, используемые в программе

Для начала работы необходимо найти портрет Лебедева Сергея Алексеевича в формате BMP (24-разрядный)(рис.2).

Также необходимо написать биографию Лебедева С.А. объёмом не менее 1000 символов без учёта пробелов.

Ниже представлены текст и изображение.

Текст:

«Sergey Alekseevich Lebedev was born in 1902 in Nizhny Novgorod, where his father was a mechanical engineer. Since childhood, he has shown an interest in science and technology. After graduating from high school in 1920, he entered the Moscow Power Engineering Institute (MEI), where he specialized in electromechanics.

Lebedev was actively engaged in scientific work at the MEI. He was one of the first in the USSR who began to study electric machines taking into account their magnetic fields. In 1928, he successfully defended his diploma and began working at the Energy Institute of the USSR Academy of Sciences, where he continued his research. In 1939, he defended his doctoral dissertation on the topic "Theory and calculation of inductive elements of electric machines which made him a leading specialist in this field.

Pioneer of Soviet computer technology:

With the outbreak of World War II, Lebedev switched his research to military topics. He was engaged in the development of anti-aircraft gun control systems, which were used in the defense of Moscow. After the war, in 1945, Lebedev led the work on the creation of the first Soviet electronic computer. This was in many ways a bold decision, since at that time Soviet science was still rather poorly developed in the field of computer technology. Lebedev enthusiastically led the team of scientists and engineers who worked on this project. In 1950, the MESM (Small Electronic Calculating Machine) was created - the first Soviet computer.

MESM was a revolutionary machine for its time. She used electronic lamps as computing elements and was able to perform arithmetic operations at high speed. In 1951 Lebedev was elected a corresponding member of the USSR Academy of Sciences. In 1953, under Lebedev's leadership, the BESM-1 (Large Electronic Calculating Machine) was created, which became one of the most powerful computers in the world. BESM-1 was able to solve problems in various fields, from atomic physics to aerodynamics.

Creation of computing centers and supercomputers:

In the 1950s and 1960s Lebedev led the creation of a number of new computers: BESM-2, BESM-3, BESM-4, BESM-6. These machines were even more powerful than their predecessors and played a key role in the development of scientific research in the USSR. Lebedev also put a lot of effort into creating computing centers in the USSR. He believed that computers should be available not only to military and scientific institutions, but also to industrial enterprises. He advocated the introduction of computer technology in various fields of the national economy.

Lebedev's contribution to the development of computer technology in the USSR is invaluable. He was one of the pioneers of this field, made a great contribution to the creation and development of the first Soviet computers, which played an important role in the development of science and technology in the USSR. Lebedev was not only an outstanding scientist, but also a talented organizer who enthusiastically promoted the introduction of computer technology in various spheres of life.

In addition to the facts described above, it is important to note:

Theoretical research: Lebedev was also engaged in theoretical research in the field of computer engineering. He developed new computer architectures, including multiprocessor systems, which were subsequently widely used in various fields.

Personnel training: Lebedev attached great importance to the training of young specialists in the field of computer technology. He led the creation of the Computing Machines Department at the Moscow Institute of Physics and Technology (MIPT), where many future outstanding scientists received their education.

Sergey Alekseevich Lebedev left a rich scientific legacy, which still influences the development of computer technology. His works and ideas largely determined the direction of development of this field

in the USSR and in the world. »

Рис. 2: Портрет Лебедева А.С.

2.3 Код программы и результат работы программы

Данный текст повторенный дважды помещается в картинку при кодировании в любое количество бит.

2.4 Описание кода

2.4.1 Lib.hs

1. encodeTextIntoImage: эта функция кодирует текст в изображение. Она принимает три аргумента:

   -
   - n: количество младших битов в каждом байте изображения, которые будут заменены битами текста
   - imageData: байты изображения
   - textData: байты текста

   Функция работает следующим образом:

   - Преобразует длину текста в 4 байта (32 бита) в формате big-endian.
   - Объединяет данные длины и текста в один ByteString.

- Преобразует байты текста в биты.
- Заменяет младшие n битов в каждом байте изображения битами текста, используя функцию replaceBitsInBytes.
- Возвращает новый ByteString с закодированным текстом.

2. decodeTextFromImage: эта функция декодирует текст из изображения. Она принимает два аргумента:

   - n: количество младших битов в каждом байте изображения, которые были использованы для кодирования текста
   - imageData: байты изображения

   Функция работает следующим образом:

   - Извлекает биты из изображения.
   - Извлекает длину текста из первых 32 бит изображения.
   - Извлекает биты текста из следующих textLength * 8 бит изображения.
   - Преобразует биты текста обратно в Text.
   - Извлекает байты изображения без текста.
   - Возвращает пару (newImageData, decodedText), где newImageData - байты изображения без текста, а decodedText - декодированный текст.

Вспомогательные функции:

- shiftChar: сдвигает символ в алфавите на заданное количество позиций.
- shiftInList: сдвигает символ в заданном списке символов на заданное количество позиций.
- bytesToBits: преобразует байты в биты.
- byteToBits: преобразует байт в список битов.
- bitsToBytes: преобразует биты в байты.
- bitsToWord8: преобразует список битов в байт.
- replaceBitsInBytes: заменяет младшие n битов в каждом байте на биты текста.
- replaceLastNBits: заменяет младшие n битов в байте.
- bitMask: создает маску для очистки младших n битов.
- bitsToValue: преобразует список битов в число.
- bitsToText: преобразует список битов в текст.

2.4.2 Main.hs

Код реализует следующие функции:

1. Чтение текста из файла biography.txt:

   - Проверяет, существует ли файл biography.txt.

   - Считывает текст из файла.

   - Подсчитывает количество символов в тексте без пробелов.

   - Проверяет, что количество символов без пробелов не менее 1000 (в коде эта проверка закомментирована).

2. Запрос сдвига для шифра Цезаря:

   - Просит пользователя ввести сдвиг для шифрования.

   - Преобразует строку в целое число.

3. Шифрование текста:

   - Использует функцию caesarEncode из модуля Lib для шифрования текста.

   - Сохраняет зашифрованный текст в файл с именем biography_сдвиг.txt.

4. Чтение изображения lebedev.bmp:

   - Проверяет, существует ли файл lebedev.bmp.

   - Считывает изображение из файла.

   - Извлекает заголовок изображения (первые 54 байта).

   - Извлекает тело изображения (остальные байты).

5. Подготовка данных текста:

   - Преобразует текст в строгий ByteString.

   - Преобразует строгий ByteString в ByteString.Lazy.

6. Создание изображений с закодированным текстом:

   - Проверяет, поместится ли текст в изображение при заданном n.

   - Использует функцию encodeTextIntoImage из модуля Lib для кодирования текста в изображение.

   - Сохраняет новое изображение с именем lebedev_сдвиг_n.bmp.

7. Запрос имени изображения для декодирования:

   - Просит пользователя ввести имя изображения для декодирования.

   - Проверяет, существует ли файл с указанным именем.

8. Извлечение сдвига и n из имени файла:

   - Разделяет имя файла на части, используя символ «_».

   - Извлекает сдвиг и n из имени файла.

9. Чтение изображения:

   - Считывает изображение из файла.

   - Извлекает тело изображения (остальные байты).

10. Декодирование текста из изображения:

    - Использует функцию decodeTextFromImage из модуля Lib для декодирования текста из изображения.

    - Выводит декодированный текст.

    - Сохраняет декодированный текст в файл с именем decoded_test.txt.

3 Результаты

На рис.3-10 изображены картинки, в которые закодирован текст.

Рис. 3: Картинка, в которой зашифрован 1 бит в каждом байте, со сдвигом Цезаря 7

Рис. 4: Картинка, в которой зашифрован 2 бита в каждом байте, со сдвигом Цезаря 7

Рис. 5: Картинка, в которой зашифрован 3 бита в каждом байте, со сдвигом Цезаря 7

Рис. 6: Картинка, в которой зашифрован 4 бита в каждом байте, со сдвигом Цезаря 7

Рис. 7: Картинка, в которой зашифрован 5 бит в каждом байте, со сдвигом Цезаря 7

Рис. 8: Картинка, в которой зашифрован 6 бит в каждом байте, со сдвигом Цезаря 7

Рис. 9: Картинка, в которой зашифрован 7 бит в каждом байте, со сдвигом Цезаря 7

Рис. 10: Картинка, в которой зашифрован 8 бит в каждом байте, со сдвигом Цезаря 7

Можно заметить, что на рис.3-6 разница заметна минимально, но на других картинках она хорошо видна в нижней части картинки.

На рис.11 изображен файл, закодированный со сдвигом. На рис.12 приведен декодированный файл.

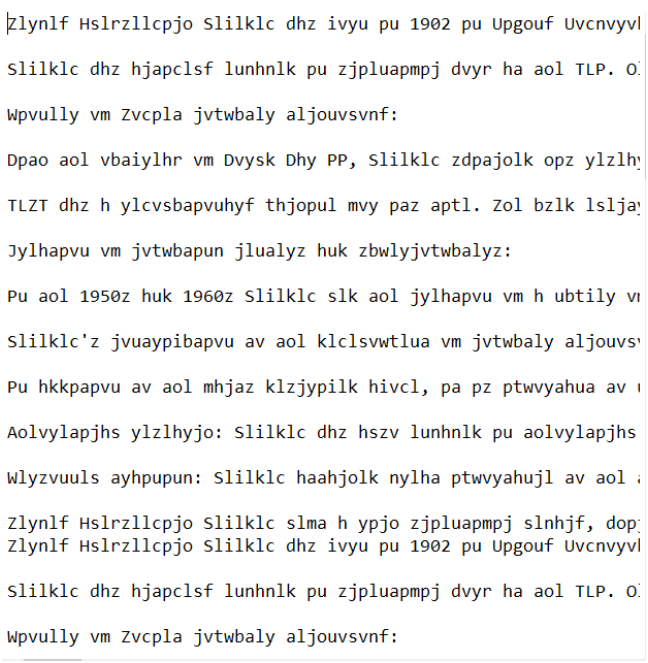

Рис. 11: Файл, закодированный со сдвигом 7

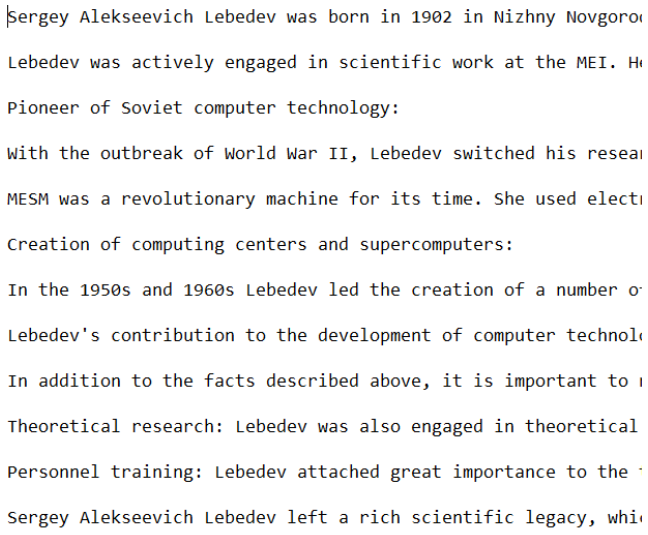

Рис. 12: Декодированный файл

По приведенным файлам видно, что сдвиг действительно 7.

Выводы

В ходе выполнения курсовой работы была разработана программа на языке Haskell, предназначенная для кодирования и декодирования текста с использованием шифра Цезаря. Программа принимает на вход 24-разрядное изображение формата BMP, в котором текст должен быть полностью помещен.

Алгоритм кодирования заключается в замене последних битов каждого байта изображения на биты из закодированного текста. Декодирование осуществляется путем извлечения закодированных битов из изображения и последующего декодирования текста с использованием информации о сдвиге.

В качестве тестовых данных были использованы текст биографии ученого Лебедева А.С. и его портрет в формате BMP. Программа успешно выполняет все поставленные задачи, подтверждая работоспособность разработанного алгоритма.

Задание выполнено в среде Visual Studio Code, GHCi, версия 9.4.8.

Список литературы

1. Новиков Ф.А., «Дискретная математика для программистов», Издательство «Питер», 2000.

2. W. Kurt. Get Programming with Haskell. Москва: ДМК, 2019.