Implementation of Reed Solomon Codes on Raspberry Pi

G Kavyashri
Dept. of Electronics and Communication
VVCE, Mysuru, Karnataka, India

Nagasanthosh M R
Dept. of Electronics and Communication
VVCE, Mysuru, Karnataka, India

Sowjanya M S
Dept. of Electronics and Communication
VVCE, Mysuru, Karnataka, India

Shruthi K
Dept. of Electronics and Communication
VVCE, Mysuru, Karnataka, India

T P Surekha
Dept. of Electronics and Communication
VVCE, Mysuru, Karnataka, India

Kavya A P
Dept. of Electronics and Communication
VVCE, Mysuru, Karnataka, India

Abstract—: In today’s scenario of ever increasing usage of wireless devices such as mobile phones and broadband modems, it is important to have robust error correction codes because the data can be corrupted over the noisy communication channels. One of such error correcting codes include Reed Solomon(RS) codes. Here, in this paper we are encrypting and decrypting using RS codes over two Raspberry Pi 3 mini computers, considering one as transmitter and the other as receiver. The stream of data is divided into blocks or code words and transmitted over the communication channel. The RS algorithm is used for any error detection and correction that occurs during the transmission and thus the decoded data is obtained at the receiver end.

Keywords— Reed Solomon codes, Encryption, Decryption Raspberry Pi 3.

I. INTRODUCTION

Nowadays, we live in a world where communication plays a very important role in our daily lives and also in economic and technological fields. For better communication, the data should not be corrupted or lost. But it can happen so over the communication channels because of noise or any other overlapping signals through the same channel. Hence, we need error detecting and correcting codes. The purpose of error correcting codes is to increase the reliability on communication channel and Signal-to-Noise ratio(SNR). There are different random error correcting codes like Reed Solomon codes, BCH (Bose, Ray-Chaudhari, and Hocquenghem) codes, Convolution codes etc. In this paper, we are considering only RS codes because of their simplicity and effectiveness in correcting random burst errors.

II. LITERATURE SURVEY

In coding theory, Reed-Solomon (RS) codes are the subset of BCH codes that are one of the most powerful known classes of linear cyclic block codes. Reed-Solomon (RS) codes are very efficient and best for correction of burst errors and have a wide range of applications in digital communication and data storage. Reed-Solomon (RS) is the most powerful technique used for error detection and correction at present [1]. RS encoder and RS decoder was designed and its functionality was verified on FPGA. An RTL (register transfer logic) code was developed for an R-S encoder that takes a 32-bit input data and produces a 48- bit output. The logic synthesis and optimization of the code was carried out using Quartus II tool. Also, an R-S decoder was developed that decodes the transmitted data [2]. The Reed-Solomon encoder has been checked for different error-correcting capabilities that is 4, 6, 8 etc. Reed-Solomon decoder for IEEE 802.16 network is synthesized on VHDL for error detection and correction. Pipelining in Reed-Solomon decoder improves the performance [3].

III. REED SOLOMON CODES

RS codes are non-binary systematic cyclic linear block codes. These codes work with symbols that’s of a byte size. They form a codeword which consists of message bits in unaltered form and also the parity bits. The codeword is formed by adding parity bits at the end of the message bits. Here, the stream of data is divided into codewords before transmission. This process of conversion of plain text or message into cipher text is known as encryption. The encrypted data is sent over the communication channel so that it can be retrieved later at the receiver end. The process of retrieving data from cipher text is known as decryption. The encoding and decoding of data is done based on RS algorithms.

A. RS encoding

RS encoding techniques were introduces by Irving S Reed and Gustave Solomon in 1960. These techniques have proved to be effective for transmission of data over unreliable communication channels. Many communication channels are unreliable and subjected to noise and thus errors can be introduced in the data. These errors need to be detected and the original data should be reconstructed through error correction. The data is sent in an encoded form from source to the receiver.

B. RS decoding

1) Syndrome Generator

It checks the presence of errors in the codeword at the receiver end. It calculates the syndrome and decides whether
an error is present or not. A valid codeword generates a syndrome polynomial with all zero co-efficients.

2) Berlekamp-Massey algorithm

The key equation solver is the main component of Reed-Solomon decoder. It provides two polynomial- error locator polynomial and error evaluator polynomial. The former contains information about the location of the erroneous symbols while the latter gives the information about the magnitude of the same.

3) Chien search

Chien search algorithm helps us find the position of the error. It checks to see if the output is zero using all the possible input values. The sum of odd values and even values are calculated and are added together. If the summation value is zero in any clock cycle, then it determines the position of the error.

4) Forney algorithm and error correction

Once the position of the error and its magnitude is known, the erroneous symbol needs to be corrected. We use Forney algorithm for this purpose. The error corrector block takes the codeword and performs XOR operation with corresponding error magnitudes. A FIFO register is used to match the order of the symbols in code words. The output of the XOR gate gives the decoder’s estimated codeword.

IV. PROPOSED SYSTEM

In our proposed system, we use RS codes for encoding and decoding data at the source and the receiver end. The RS algorithm used divides the message signal into six blocks out of which four blocks contain actual data and the other two blocks contain the parity bits. These blocks of data (encoded data) are sent through the communication channel. Even if the channel is unreliable and message gets corrupted, RS code detects and corrects these errors. This developed algorithm can retrieve the data even if two of those six blocks are lost over the channel.

IV. SIMULATION RESULTS

The simulation results that were obtained by us are shown below.

We have used Raspberry Pi 3, mini computers to implement our proposed system. We have designed this system using Java. The requests from user will be in the JSON file format. This file is given to encoder to encode and generate the codeword. That codeword is transmitted through the communication channel to its destination. The receiver at the destination decodes the codeword, checks for errors that might be added during the transmission and corrects them using the RS codes. The decoder then sends the codeword to the request handler to process the user request. The request handler accepts the request and sends it to the corresponding Java script stored on the server in the encoded format. This code is then verified by the RS decoder. The complete procedure is shown in the figure.

Fig. 1. Raspberry Pi 3

Fig. 2. Encoding and decoding using RS Codes

Fig. 3. File successfully encoded and sent

Fig. 4. File successfully decoded
V. CONCLUSION AND FUTURE SCOPE

This paper describes the implementation of RS Codes on Raspberry Pi 3. Error detection and correction techniques are used for reliable communication. The Raspberry Pi is used as source at one end and receiver at the other end. The source send the encoded message as codewords and these codewords are decoded at the receiver end using RS encoding and decoding techniques. The Java programming language is used to write the code and is implemented on Raspberry Pi 3. This algorithm divides the message into six blocks and transmits them. Decoder decodes it and retrieves original message even if two blocks are lost during transmission. This algorithm can be further implemented for higher number of data symbols and for other communication applications.

ACKNOWLEDGMENT

Authors wish to express sincere gratitude to our beloved Principal, Dr. B Sadashive Gowda, Vidyavardhaka College of Engineering, Mysuru. Our sincere thanks to Dr. D J Ravi, Professor and Head, Dept. of Electronics and Communication Engineering, VVCE. We express our sincere gratitude to our guides, Dr. T P Surekha, Professor and Ms. Kavya A P, Assistant Professor, Dept. of Electronics and Communication Engineering, VVCE, Mysuru.

REFERENCES