ASIC Implementation of Convolutional Encoder and Viterbi Decoder Based on DNA Cryptography

P. E. Rani¹, G. Ravi Kanth²
M.Tech Student¹, Professor²
Department of Electronics & Communication Engineering
BVC College of Engineering, Rajahmundry, India

Abstract:
In the convolutional operation encodes the transmitted operation encodes the transmitting signal some dispensable information, thus improving the channel data capacity. Viterbi algorithm is commonly used for sensitive models including the decoding the convolutional codes widely used in communication systems such as Satellite communication, Relays and Local wireless channel network. In additional, Viterbi algorithm is used to automatic speech generation and also storage devices as well as application. Cryptography is a scheme used to hide and secure the information without any loss. We have developed a security system of convolutional encoder and Viterbi decoder using DNA cryptography. DNA is used for cryptography due to encryption of convolutional encoder and decryption of Viterbi. Viterbi decoder is one used blocks in data communication systems. Optimizing its word length causes a substantial reduction within the chip space and decryption delay. FPGA synthesis reports the Xilinx tool of using the Viterx-6 family.

Index Terms: Convolution Encoder, Viterbi Decoder, Cryptography, DNA.

I. INTRODUCTION

In the Viterbi algorithm is cost effective. It used in communication systems to decode the convolutional codes. This paper explores that convolutional encoder and Viterbi decoder implementation design [1] using DNA cryptography. This assembled to explain the design of convolutional encoder and decoder for constraint length (K) with code rate ½ describes the block diagram for implementing the Viterbi decoder [2], [3]. The importance of Viterbi algorithm’s convolutional codes decoding should not depend on the specific distribution of zeros and ones in the input messages as they are linear. Specific implementation of the Viterbi algorithm [4] during the sub blocks are Branch Metric Unit, Add Compare Select Unit and Survivor Path. However, it was identified to demonstrate the decoding performance that depends on the proportion of elements in the input message bits. In addition, the Viterbi decoder is used in high speed (SERDES) implementations that have critical latency constraints. Convolutional codes are mainly defined using two constants: code rate and constraint length. The code rate(r) as k / n is a count of bits in the convolution encoder (k) to the no of symbols generate by channel of the convolutional encoder (n) in the encoding cycle. The parameter of constraint k denotes length of the convolutional encoder and indicates that many k bits stage are available to give the combination logic producing the o/p symbols [5].

There are three major components of Viterbi decoders: branch metric unit (BMU), Add-compare-select (ACS) unit and survivor path (SMU) unit. In the Viterbi decoding memory path changes degrade the range of encoding codes. When the relevant state of BMU is the received and expected state of information to the add compare select is the forward logic, when the loop convert the smallest path to find and path arrival at ACS unit. In survivor path to make decision at the Viterbi decoder.

II. RELEVANT IMPLEMENTATION DETAILS OF CONVOLUTIONAL AND VITERBI ALGORITHM

In the encode data of convolutional encoder into code rate of value by using the shifting data at the register to register and output data encryption. Here shift register used to modulo-2 adder encrypt data. Viterbi algorithm architecture is commonly used in the decoding of convolution codes.

In the presence of very large-scale integration (VLSI) defects, erroneous outputs may occur which degrade the decoding convolutional codes [9]. Each path connecting the output to a convolutional encoder's input is characterized in terms of its impulse response. It is the response of that path to a symbol applied to its input, with each flip flop in the encoder initially set to zero [10].

Where the selection DNA module encode code of convolutional encoder and sequence of message bits and the decrypted the data to same plaint text into cipher text format of Viterbi decoder modules. The information is changing the by using DNA cryptography. Each path is then characterized in terms of a generator polynomial which is the unit delay transform of the impulse response[11].

The state diagram for the (2, 1, 3) code where 2 represents the encoder's output bit, 1 represents the encoder's input bit, and 3 represents the constraint length in the presentation of the Viterbi algorithm. This is the results of the simulation and implementation of FPGA / ASIC [12]. Figure 1 is showing the Encryption and Decryption Flow Chart.
In the Design flow encryption data input size is 8 bit by using convolutional encoder convert into 16 bit, where this 16-bit gives the DNA by using ASCII converter. In decryption 16-bit data convert into 8-bit by using Viterbi decoder. Figure 1 represents the architecture of the block diagram.

**A. Convolutional Encoder**

When the data is developed, to reproduce the sequence bits to form Viterbi decoder were the contribution of convolutional encoder [10]. The convolutional algorithm shown in below steps.

1. Initially, to choose the message bit in the input side at current state and previous state bits to save the number.
2. By shifting the bits, current state during register to register level and calculation of g1 and g2 using XOR operation this is obtain[7] until the new currently save the message bits. Repeat the process up to the change the message bits.
3. In the convolutional encoder most likely encoded by the message bit to change from every predecessor state of the Input bits.

The output sequence obtained using the lower modulo-2 adder O/P2 is (00100110). The combined output sequences of the two modulo-2 adders are given by \{0001110000100\}. For a sample input sequence: 00101101 and the encoder output sequence is obtained as: 00 00 11 10 00 10 00 00. Figure 2 represents the block diagram for convolutional encoder. In the comprehension of its task represented in three diverse graphical ways of the convolutional encoder are state diagram, Trellis diagram and Tree diagram. The state diagram for the code is given in where [9] represents the output bit of the encoder, represents the input bit to the encoder and represents the constraint length. The Convolutional Algorithm Steps shown in figure 3.

**B. Viterbi Decoder**

In the Viterbi decoder, where every pair of bit is given to the decoder at the sequence of convolutional encoder. Figure 4 shows the block diagram of the Viterbi decoder. When the Viterbi decoder block diagram briefly explain that branch metric unit connected to the Add compare select unit and again connected to the path metric unit here, the loop structure represented and form the ACS unit[4] In the received ACS unit to form the Survivor path during that the method to produce the decoded output of the Viterbi algorithm.

The output sequence to form the timing analysis and delay of the path to decoded information. In the Viterbi decoder blocks to explain in detail that BM at time t = 1 due to add compare select to form the path metric at smallest count of the trellis to find the
survivor path at the decision level of the information. In these Major Blocks are used in the Viterbi algorithm are Branch Metric Unit (BMU), Add Compare Select Unit (ACSU), and Survivor Path Unit (SPU).

**a. Branch metric**
The principal unit of Hamming distance due to the normal unit and original unit of the message bits of the branch metric unit. Their separation technique of the branch metric unit as certain utilized the hamming distance. In the BM shows the time at t=1. Here hamming distance calculation to branch metric unit. The branch metric unit number of bits shown in above figure 4. The principal unit of the received information to the transmitter from determined contrasted yields.

**b. Add Compare Select Unit**
In the add compare select to process the sub modules on the path metric unit to generate the trellis of the decision. When the stages of the path has two stages that measurements going to the current state. In path metric to choose the transmitted data to the add compare select and loop operation on the stage. In the adding themselves to characterized the particular path. When the code trellis of shortest path number at the coding bits. In the components are ACS and PMU on the ACSU.

**c. Survivor path**
In the survivor path the decoded data stored to add compare select unit. When the decision making to current data flow into the register level path of the ACS unit. In the next level of the survivor unit to produce the input to ACS output. When the significantly use the data to exchange method. More time taken to convert the register level exchange.

**C. DNA Cryptography**
When the DNA con store the utilized data in the form of ASCII codes and transmit the information in the pairs of three cipher text of DNA. Where the data of RNA and DNA are in same base sequence like A-0, C-1, G-2, T-3. In the code values of the DNA represents the 00,01,10,11 sequence of bits. Here the A, G, C, T denoted as Adenine, Thymine, Cytosine, Guanine. DNA has double-helix structure [15]. When the Plain text of information is converted into the cipher text to produce output it acts as cryptography, where cryptography used to secure the data without any loss of information at the plain text of the data to modified the original data at the ASCII codes of message bits.

<table>
<thead>
<tr>
<th>DNA Structure</th>
<th>Binary Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>00</td>
</tr>
<tr>
<td>C</td>
<td>01</td>
</tr>
<tr>
<td>G</td>
<td>10</td>
</tr>
<tr>
<td>T</td>
<td>11</td>
</tr>
</tbody>
</table>

In this DNA used to convert the message bits of convolutional encoder of the encoded data. In this paper represented the secure data to encryption and decryption information providing the message bit by using the cryptography. In the cryptography Alice the data plain text by using ASCII code into the cipher text, here key generation to secure information at the possible calculations to developing figure of DNA. When the symbols represented in the data, once the information conveying the results easily to secure. Cryptography to recreate information is privacy and Viterbi decoder to form the decoded output.

**III. FPGA SYNTHESIS REPORT AND RESULT ANALYSIS**
Field programmable Gate Array (FPGA) are using to critical part of every system. For this DNA cryptography design Here used in Xilinx Vivado. We developed total hardware using in Verilog HDL. Figure 7[a], [b], [c] are shows the RTL (FPGA) schematic view of convolutional encoder, DNA Cryptography and Viterbi decoder modules. In the Figure 8, Figure 9, Figure10 are the simulation results of convolutional encoder, DNA Cryptography and Viterbi decoder modules. The encryption and decryption FPGA device utilization is used as LUT are 8 and I/O are 32 used in Convolutional Encoder, LUT are 23 and I/O are 80 used in DNA Cryptography, LUT are 23 and I/O are 40 used in Viterbi decoder.
Figure 7. RTL Schematic View [a] Convolutional Encoder [b] DNA Cryptography [c] Viterbi Decoder

Figure 8. Convolutional Encoder Simulation Timing Diagram

Figure 9. DNA Cryptography Simulation Timing Diagram
IV. CONCLUSION

We have developed a DNA based cryptography using convolutional Encoder and Viterbi Decoder, that increase complexity in each round thus it can increase the security. Time taken for encryption and decryption of data procedure is efficient on the grounds of basic strategies are utilized. So that it increases the efficiency and gives high accuracy. By using same security algorithm, we are optimizing the resource utilization. To implement this designed we have used Verilog HDL. The total process is tested on FPGA Viterx-6 Kit. The total power consumed by encryption module is 3.86 W. The total power consumed by decryption module is 2.11W. The total delay in convolutional encoder is 0.837ns and total delay in Viterbi decoder is 0.345ns. For medical images data analysis this algorithm secures the data. New methodologies can help this algorithm in future to diminish the activity while keeping up the adequate level of security. In this chapter we clearly observe the results of this project by using Xilinx software and here the results are simulation, RTL schematic views and synthesis reports.

V. REFERENCES


