IJMTST is UGC Approved Journal with Journal Id: 43137

International Journal for Modern Trends in Science and Technology, 8(S05):75-82, 2022

ISSN: 2455-3778 online
DOI: https://doi.org/10.46501/IJMTST08S0513
Available online at: https://www.ijmtst.com/vol8si05.html

Low Power DNA Cryptography Based 64 Bit ASIC Implementation ff Convolution Encoder and Viterbi Decoder

K.V.Acharyulu | B.Manikanta| B.Deepika| B.Sravan Kumar

Department of Electronics and Communication Engineering, Godavari Institute of Engineering and Technology(A), JNTUK, Kakinada.

To Cite this Article
K.V.Acharyulu, B.Manikanta, B.Deepika and B.Sravan Kumar. Low Power DNA Cryptography Based 64 Bit ASIC Implementation ff Convolution Encoder and Viterbi Decoder. International Journal for Modern Trends in Science and Technology 2022, 8(S05), pp. 75-82. https://doi.org/10.46501/IJMTST08S0513

Article Info
Received: 26 April 2022; Accepted: 24 May 2022; Published: 30 May 2022.

ABSTRACT

The transmitted signal is encoded with some non-essential information in the convolutional process, hence boosting the channel data capacity. For sensitive models, the Viterbi method is often used. Convolutional code decoding is commonly employed in communication systems such as satellite communication, relays, and local wireless channel networks. Furthermore, the Viterbi algorithm is employed in artificial speech generation as well as storage devices. Cryptography is a technique used to hide and secure information without any data loss. Using DNA cryptography, we have developed a convolutional encoder and a Viterbi decoder security system.DNA cipher is used to encode the encoded message at the convolutional encoder and decode the message at the Viterbi decoder. The Viterbi decoder is utilized in data communication system blocks. The word length is optimized, resulting in a significant reduction in chip area and decryption delay. The design and implementation of this algorithm have been done in Verilog HDL using Xilinx ISE design Suite14.7. The Xilinx tool for FPGA synthesis employs the Virtex-6 family.

KEYWORDS: Convolution encoder, Viterbi decoder, DNA Cryptography, Encryption, Decryption, FPGA.

1.INTRODUCTION

A Communication System transmits information from source to destination via a channel that can be wired or wireless. This paper mainly focuses on data transmission through wireless channels. Information transmission over wireless channels is hampered by attenuation, distortion, interference, and noise, which impairs the receiver's ability to receive accurate information. Convolutional coding is a widely used error-correcting coding method in digital communications. The transmitted signal is encoded with some non-essential information in the convolutional process, hence boosting the channel data capacity. The Viterbi algorithm is a well-known method for decoding convolutionally coded messages. This paper investigates the design of a convolutional encoder and Viterbi decoder using DNA cryptography. Convolutional coding is used in a variety of communication systems, including deep space communications and wireless communications. This project can be implemented using FPGA or ASIC.ASIC refers to Application Specific Integrated Circuit. Implementing this architecture using an ASIC is more efficient in terms of power and performance. On the other hand, ASIC is a fixed design that does not allow for much operational flexibility. The significance of the Viterbi algorithm's convolutional code decoding should

not be dependent on the specific distribution of zeros and ones in the input messages because they are linear. The Viterbi algorithm is implemented in the subblocks as Branch Metric Unit, Add Compare Select Unit, Path Metric Unit, and Survivor Path Memory Unit. However, it was identified to demonstrate the decoding performance that is dependent on the proportion of elements in the input message bits. Furthermore, the Viterbi decoder is used in high-speed implementations with critical latency constraints.

2. LITERATURE SURVEY

Anuj Sai and Kiran Kumar [1] have proposed the design and implementation of a convolution encoder and Viterbi decoder with a code rate of ½. They have implemented the design in FPGA. They sent the 8-bit message information through a noisy channel which was Additive White Gaussian Noise Channel. Out of all the error-correcting codes these convolution codes exhibit higher efficiency. This work mainly concentrates on the data transmission over a noisy channel. This FPGA provides more operational flexibility but it consumes a bit of high power which results in the degradation of efficiency. This paper was published in the International Journal of Scientific & Engineering Research in March 2018. This design was implemented in Verilog HDL on Xilinx ISE Design Suite 13.1 for the FPGA Artix-7 family.
Hari Kishore and Deepthi [2] have suggested a High Secured Low Power Advanced Encryption Standard (AES) Implementation with DNA Cryptography. In this Paper the security of the information has been provided with AES encryption standards using DNA Cryptography. The information in form of 128 bits has been converted into ciphertext using the DNA elements such as A, C, G, T, and also key has been passed so that the information will be secured.
Fazal Noorbasha, G.Jhansi[3] have proposed Asic Implementation of Convolution Encoder and Viterbi decoder based on Cryptography System. In this paper, they have transmitted 8-bit information securely and without any errors. The 8-bit information is encoded and also converted into ciphertext and at the receiver, the information is decoded but the major problem is the power consumption is more, and also bit transmission is less.

3. EXISTING METHOD

While we are transmitting information from source to destination we majorly consider two parameters which are the security and error tolerance of the system. When the information is affected by the noise the information gets corrupted. So in this case encoders are used. The encoder will add the redundant bits to the message. An encoder is likely to be found wherever motion precision is critical. It can be found in a wide range of applications, from mission-critical applications in harsh environments to routine workplace applications that require uncompromised repeatability. A binary code of N digits can store 2N distinct elements of coded information. Encoders convert 2N lines of input into an N-bit code, and Decoders decode the N-bit code back into 2N lines. An encoder is a combinational circuit that converts binary information in the form of 2N input lines into N output lines that represent the input's N bit code. A decoder performs the inverse operation of an encoder. It is a combinational circuit that converts n input lines into 2n output lines.
However, much of the early work has focused on punctured convolutional codes and the BCJR method, which provide lower delay, power, and accuracy. However, the suggested convolutional encoder and Viterbi algorithm [4] are approximate and will provide fixed accuracy in the runtime. This reconfigurable accuracy is very important in providing better quality services while conducting the operation, therefore by lowering the system's accuracy, other variables like power and delay are also lowered. The general-purpose processor can be utilized in both exact and approximate modes. We're mostly concerned with speed, power consumption, and precision.
Nowadays, data transformation and data security are crucial, so we are motivated to overcome the shortcomings of previous algorithms, encoders, and decoders, and thus improve the features of the data. By utilizing communication systems to decode the convolutional codes, the convolutional encoder and Viterbi decoder implementation were designed using DNA cryptography[5]. This assembled to explain the design of convolutional encoder and decode for constraint length (K) with code rate 1/2 describes the implementation of the Viterbi decoder.

4.PROPOSED METHOD

Data Security and Data Transmission are two main parameters of the system when we are transferring information from source to destination [6]. This can be achieved by using the proposed methodology. The proposed method consists of three basic steps which are convolution encoding, DNA cryptography, and Viterbi decoding. Figure1 shows the block diagram of the proposed method.

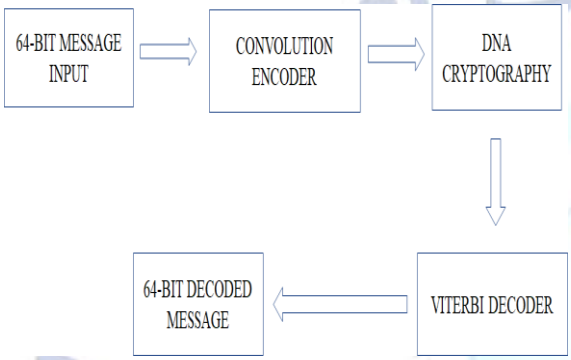

Figure 1: Block Diagram Of The Proposed Method

The block diagram gives a brief description of the proposed system. In this, the 64-bit message input is convoluted with some redundant information in the convolution in the encoding process and hence the 64-bit message is converted into 128 bit encoded message. After the convolution process, the encoded message is passed to the DNA cryptography process and here the binary text is converted into ciphertext, at the receiver, the ciphertext is again decoded and this decoded message is given as input to the Viterbi decoder and finally at the output of decoder the 64-bit message is obtained.

CONVOLUTION ENCODER:

Convolutional codes are error-correcting codes in which indefinite-length data streams are encoded before transmission over noisy channels[7]. Convolution codes were first introduced by P.Elias in 1955.Convolutional codes are excellent at preventing random errors in digital data transmission caused by any noise source. It achieves error-free transmission by adding sufficient redundancy to the source symbols. Convolution codes are mainly dependent upon two parameters which are code rate and constraint length.

The code rate (k/n) is defined as the ratio of input symbols (k) to the output symbols (n). constraint length (m) is the number of shift registers that are used[8]. The state diagram can be represented by (n,k,m). In this paper, we are designing the convolution encoder with code rate (1/2) shown in figure 2 and constraint length (3). The state diagram can be expressed in terms of (n,k,m). It can be represented as (2,1,3) where 2 is the no of output symbols and 1 represents the number of input symbols and 3 is the constraint length.

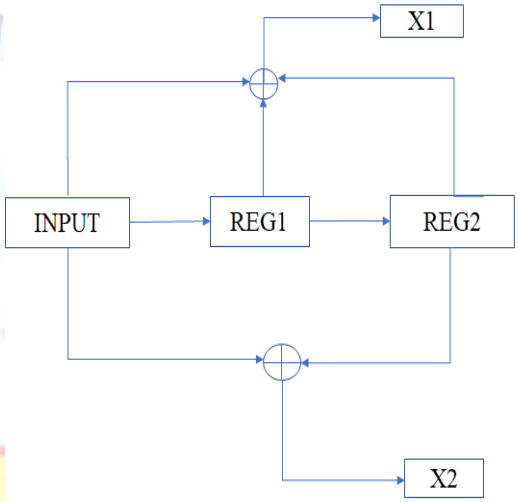

Figure 2: Convolution Encoder With Code Rate(1/2)

The algorithm for the convolution encoder can be expressed as follows:

Step1:Initially the previous registers are marked as zeroes and also the input bits are passed sequentially

Step2:When ever the input bits are passed then we get the two outputs x1 and x2 where x1=input^reg1^reg2 and also x2=input^reg2.

Step3:After obtaining the outputs the shiting operations take place and again the next input bit enters into the input register and this process continues till the input message completes.

Here figure3 describes the convolution encoder design flow.

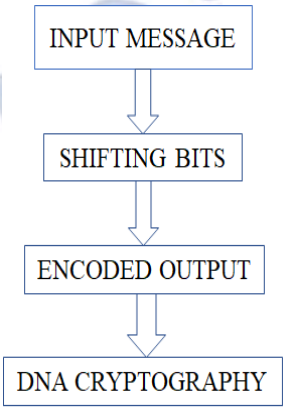

Figure3: Convolution Encoder Design Flow

Hence we have transmitted the 64-bit message to the convolution encoder and obtained 128 bit encoded message as the output.

DNA CRYPTOGRAPHY

Cryptography is the process of hiding information in the form of ciphertext. It helps in increasing data security.Cryptography is used to secure data without causing data loss. Cryptography can be divided into two types which were Symmetric Key Cryptography, Hash Function, and Asymmetric Key Cryptography.DNA Cryptography belongs to Symmetric-key Cryptography.DNA Cryptography is the process of securing and hiding information in terms of DNA sequence.

DNA refers to Deoxyribo Nucleic Acid which is the important pigment present in living beings. The DNA contains the necessary genetic information that may be used to produce other cells such as proteins and RNA. DNA is a double helix structure formed of nucleotides that are made up of two strands that are coiled to each other which is shown in figure4 [9].DNA Strand is mainly made up of 4 Nitrogen Bases namely Adenine (A), Thymine (T), Guanine (G), and Cytosine (C).

DNA can be used to store the information in the form of ASCII codes and can be used to transfer the information or data in the terms of ciphertext of DNA sequence. Generally, Adenine(A) can be assigned to 1. Similarly for other components Cytosine(C) -2, Guanine(G)-3, and Thymine(T) -4.The encoded message here is grouped into two bits and transmits information in terms of ACGT pairs.

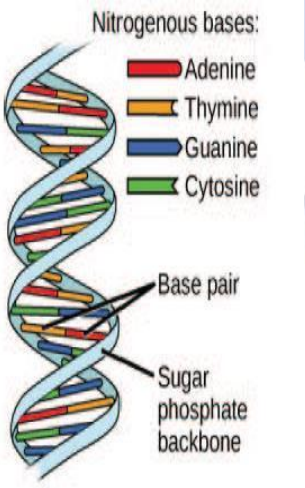

Figure4: DNA Structure

DNA COMPONENT	BINARY VALUE
A	00
C	01
G	10
T	11

Figure5: DNA Cryptography Process

Here Adenine and Thymine form as pairs and also Guanine and Cytosine form as pairs.[10] Polymerase Chain Reaction (PCR) is a method of DNA replication, amplifying a single or several copies to generate millions of duplicates

duplicates of the DNA sequence Initially, the encoded message is sent through the DNA process and later these are encrypted in the terms of DNA sequence which is in the combination of 0's and 1's. The two binary digits are grouped and assigned to the pigment as mentioned in figure5 such that A-00, C-01, G-10, and T-11. Hence in the encryption process, the 128-bit encoded message is encrypted into ciphertext and this is passed to the channel or medium. At the receiver, this encrypted ciphertext is converted to the encoded message and this is given as input to the Viterbi decoder.

Using cryptography, the work is implemented to secure the data to encryption and decryption [11], information delivering the message bit. Cryptography generally converts plain text data into encrypted text by employing ASCII code, and key creation is used to protect information at the potential calculations to produce a figure of DNA. When the symbols in the data are represented, the information transmitting the results is easily safe. Cryptography is used to regenerate information to maintain privacy, and a Viterbi decoder is used to generate the decoded output.

VITERBI DECODER

In the decoding of convolution codes [12], the Viterbi algorithm is widely used. The Viterbi method is the most likely decoding algorithm for convolutional codes. It uses the trellis diagram to decode the convolution codes. Figure6 represents the trellis diagram with four different states a,b,c, and d.

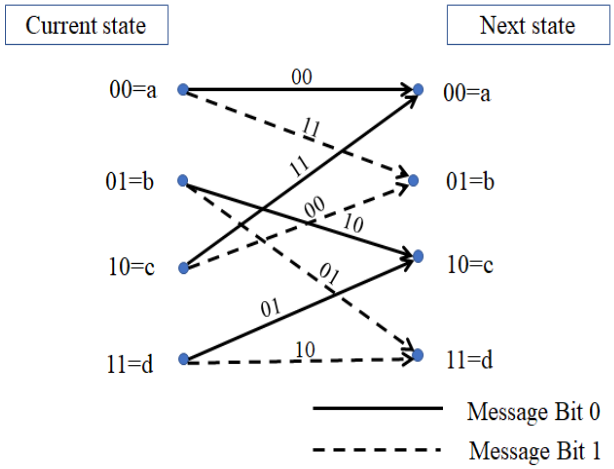

Figure6: Trellis Diagram

A Viterbi decoder is used to decode a bitstream encoded with FEC based on a Convolutional code. [13] The block diagram of a Viterbi decoder is shown in figure 7 . It is made up of the following functional units: the Branch Metric Unit, the Add Compare Select Unit, the Path Metric Unit, and the Survivor Memory Unit.

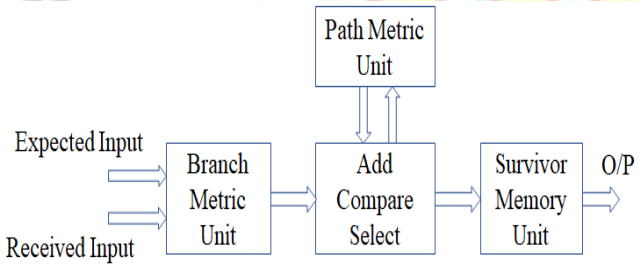

Figure7: Block Diagram of Viterbi Decoder

Branch Metric Unit

It is the first Section that is present in the Viterbi decoder. The Branch Metric unit compares the received data to the expected code and counts the number of bits that differ from the expected data to the received data, which is known as the Hamming distance [14]. As a result, Hamming distance is used to compute branch metrics.

Add Compare Select Unit

In this unit, adders compute the partial path metric of each branch and transmit it to a comparator, which compares two path metrics. Finally, the selector chooses a specific branch that has the least Hamming distance [15]. The new partial path metric updates the metric, and the survivor path recording block saves the survivor path.

Path Metric Unit

The path metric unit also consists of the Add compare and select unit. The comparator compares partial path metrics, and the selector chooses the branch metric. That is, the smaller value is chosen by the selector. The other unit, which was the path metric computation unit, calculates the path metrics of a step by adding the branch metrics, combined with a received symbol, to the path metrics from the earlier stage of the trellis.

Survivor Memory Unit

There are two ways to design a Survivor Memory Management Unit (SMU). The first is the Register Exchange method, and the second is the Traceback method. Each state is assigned a register using the Register Exchange approach. The register stores the decoded output sequence from the initial state to the final state, which is the same as the initial state. The Euclidean distance can be used to implement this method.The storage in the Trace Back unit method can be implemented as RAM and is referred to as the path memory. After processing at least L branches, the trellis connections are recollected in reverse order and the path is traced back through the trellis diagram. This is accomplished through the use of Hamming distance.

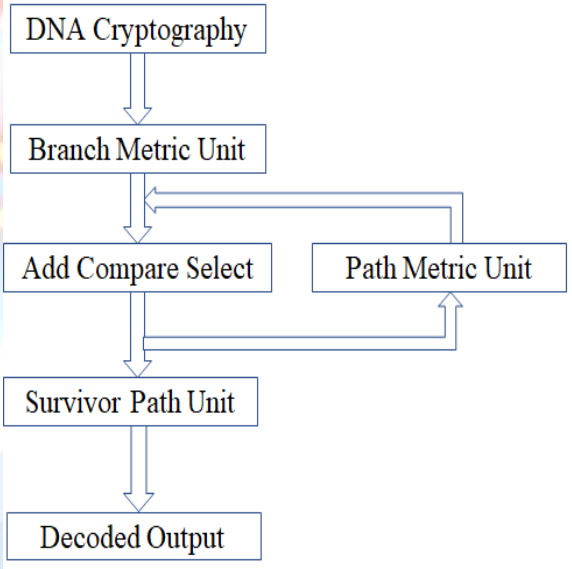

Figure8: Design Flow of Viterbi Decoder

Figure8 discusses the design flow of the Viterbi decoder [16]. The Viterbi algorithm can be briefly explained in the steps below:

Step1: Calculate the Hamming distance from the Branch Metric Unit and then this is passed to the Path Metric Unit.

Step2:In the Path Metric Unit, the adders and comparators select the path which has the least metric values and this is passed to the Survivor memory unit.

Step3: After that, the path is stored in the memory and this process continues until the stages in the trellis get

completed.By using the traceback unit the path is obtained and hence the corresponding message at the branches is obtained at the output of the Viterbi decoder.

5.RESULTS

The design is synthesized on the FPGA Virtex-6 family. The circuit is designed and implemented on Xilinx ISE design Suite 14.7 using Verilog HDL Language [17]. Figure 9represents the RTL Schematic view of Convolution Encoder, DNA Cryptography, and Viterbi Decoder Modules.Figure10 represents the simulation results of the design and also Figure11 represents the power report [18].

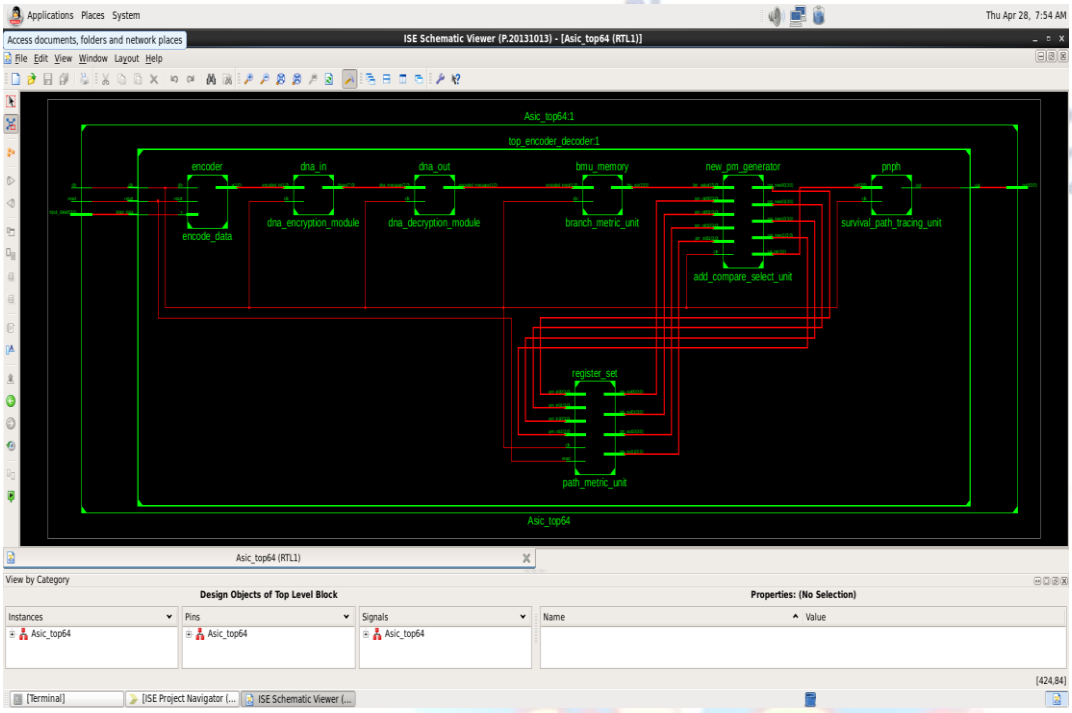

Figure 9: RTL Schematic View of Convolution Encoder, DNA Cryptography, and Viterbi Decoder

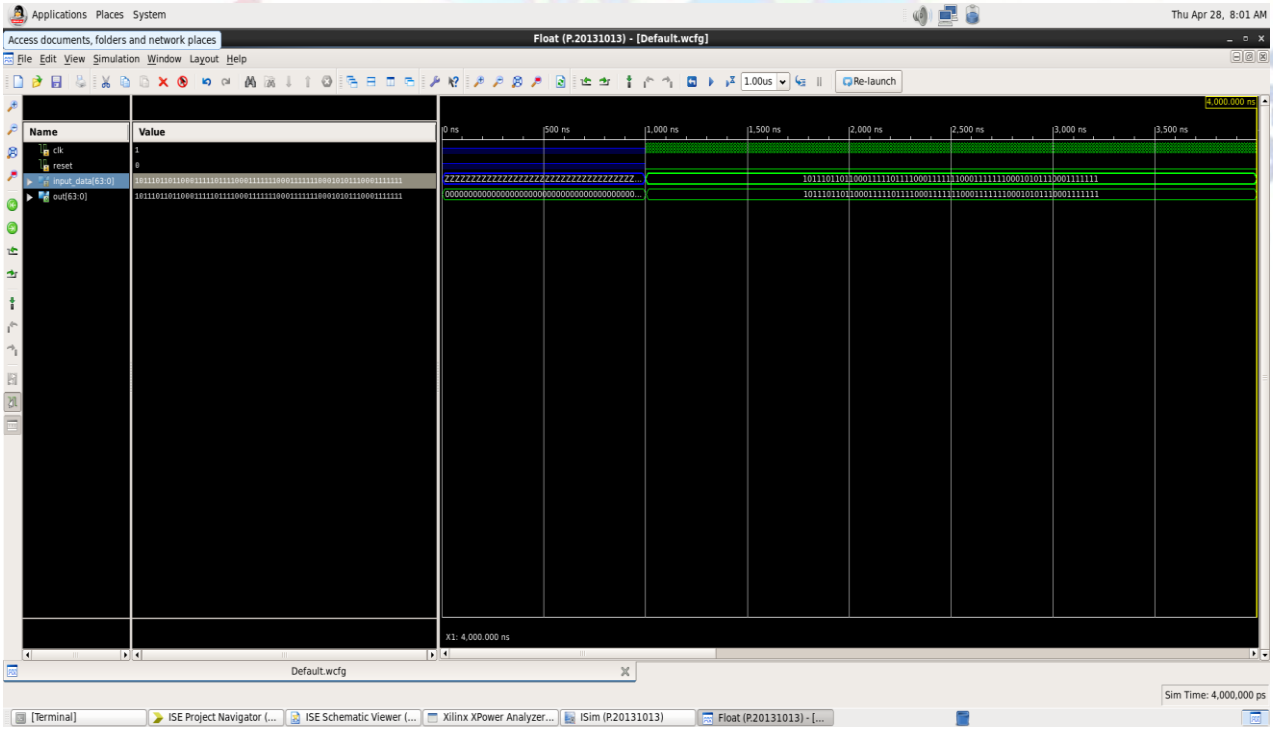

Figure10: Simulation Timing Diagram

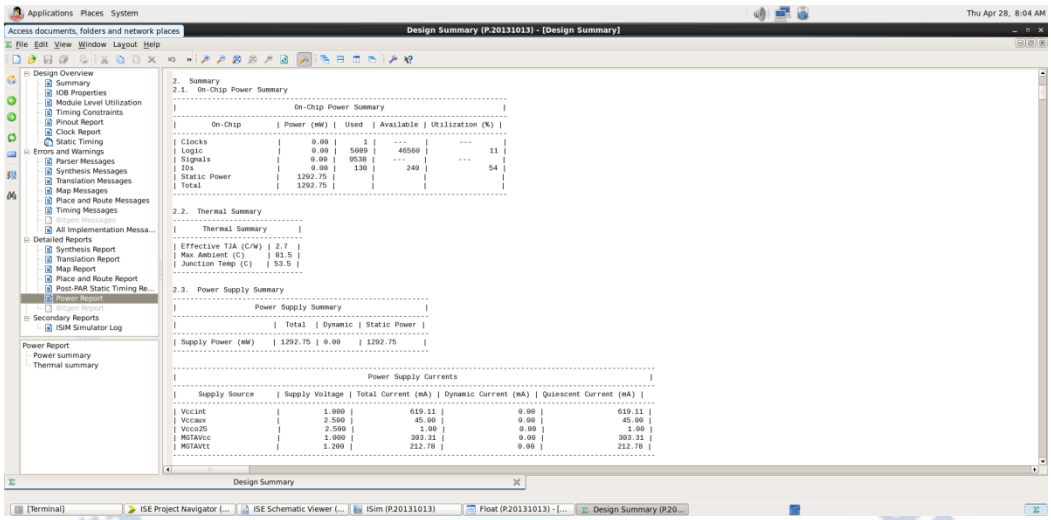

Figure11: Power Report

6. CONCLUSION

In this paper, we have designed an integrated circuit of the Convolution encoder with a Viterbi decoder using DNA Cryptography which will be used for secure data communication purposes. Here we have used a Convolution encoder with a code rate (1/2) have been simulated using Verilog HDL in Xilinx ISE Design Suite 14.7. The encoding and decoding increase the complexity hence the security of the information will also be increased. Because simple methodologies are used, the time spent on data encryption and decryption is efficient. As a result, the efficiencies are high, and accuracy is good. Using this methodology we are optimizing resource utilization. In the figure10 the power report of this design or model is calculated and the overall power for the encrypted and decrypted module is 1.3 W.

which consumes less power than the existing model. This model can be useful in various communication systems such as Satellite communications, Deep Space communications, Radio communications, Aircraft Navigation systems, Military applications, etc.

Conflict of interest statement

Authors declare that they do not have any conflict of interest.

REFERENCES

[1] Anuj Sai, Kiran Kumar, Vamshi Krishna Reddy, and Shiva Nagender Rao " FPGA Design and Implementation of Convolution Encoder and Viterbi Decoder " International Journal of Scientific & Engineering Research, March-2018 ISSN 2229-5518.

[2] K Deepthi, K Hari Kishore, Fazal Noorbasha, and G.Jhansi " Implementation of High Secured Low Power Advanced Encryption Standard (AES) Implementation with DNA Cryptography " International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-8 Issue-6S, April 2019.

[3] Fazal Noorbasha, G.Jhansi, K.Deepthi, and K Hari Kishore " ASIC Implementation of Convolution Encoder and Viterbi Decoder Based Cryptography System " International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-8 Issue-6S, April 2019.

[4] M. Reshma Reddy and P. Tirumala Rao " FPGA Implementation of Convolutional Encoder and Viterbi Decoder using VHDL " International Journal of Scientific Engineering and Technology Research ISSN 2319-8885 Vol.03, Issue.46 December-2014.

[5] Ahmed Y. Yousuf, and Haider Hadi Abbas " TEXT ENCRYPTION AND DECRYPTION USING FIVE LEVELS DNA BASED ALGORITHM " International Journal of Advanced Science and Technology " Vol. 29, No. 3s, (2020), pp. 104-108.

[6] Bineeta Soreg and Saurabh Kumar "Efficient Implementation of Convolution Encoder and Viterbi decoder" 2013 International Conference on Circuits, Power and Computing Technologies.

[7] B.Swetha Reddy and K.Srinivas "FPGA Implementation of Convolutional Encoder and Adaptive Viterbi Decoder" International Journal of Scientific Engineering and Technology Research ISSN 2319-8885 October-2014.

[8] Pravallika, Suryaprakash and Vijay Bhaskar " HDL Implementation of convolution encoder and Viterbi decoder" International Journal of Engineering Research & Technology (IJERT) Vol. 1 Issue 5, July - 2012 ISSN: 2278-0181.

[9] Karthiga S, and Murugavalli E " DNA CRYPTOGRAPHY " International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056 Volume: 05 Issue: 03 | Mar-2018.

[10] Anuj Kumar " Data Security and Privacy using DNA Cryptography and AES Method in Cloud Computing " 2021 Fifth International Conference on I-SMAC.

[11] M. Manasa, R. Tulasi Gouthami, D. Hari Priya, N. Prashanth, "FPGA Implementation Of Cryptographic Systems For Symmetric Encryption", Journal of Theoretical and Applied Information Technology, 2017.

[12] Ranjitha S, Divya Preethi K, Megha K, and T Anusha Lalitha "An Efficient FPGA Implementation of Convolutional Encoder and Viterbi Decoder for DSP Applications " International Journal of Engineering Research & Technology (IJERT) ISSN: 2278-0181.

[13] Nimisha and Prakash Biswagar, "Viterbi Algorithm Based Bluetooth Low Energy Receiver for IoT", 2nd IEEE International Conference in Electronics Information & Communication Technology (RTEICT), May 2017.

[14] Habib, S. Sawitzki, " Design Space Exploration of Hard-Decision Viterbi Decoding: Algorithm and VLSI Implementation" IEEE Tran. on Very Large Scale Integration (VLSI) Systems, May 2010.

[15] Wong, Y.S. et.al "Implementation of the convolutional encoder and Viterbi decoder using VHDL" IEEE Tran. on Inform. Theory, Nov. 2009.

[16] S.W. Shaker, Salwa Hussien Elramly and Khaled Ali Shehata, "FPGA Implementation of a Configurable Viterbi Decoder for Software Radio Receiver", Autotestcon, IEEE, July 2009.

[17] K.Santhosh Kumar and M.V.H. Bhaskara Murthy " FPGA Implementation of Viterbi Algorithm for Decoding of Convolution Codes " IOSR Journal of VLSI and Signal Processing (IOSR-JVSP) Volume 4, Issue 5, Ver. I (Sep-Oct. 2014).

[18] P.Rani and G.Ravi Kanth " ASIC Implementation of Convolutional Encoder and Viterbi Decoder Based on DNA Cryptography " International Journal of Engineering Science and Computing 2020 ISSN 2321 336.