Journal of Positive Sciences (JPS) **eISSN: 2582-9351, https://positive-sciences.com** **JPS. 2021 Jun; 1(3): 1-5**

Article info **Research Article**
Received on: 23.05.2021
Accepted on: 27.06.2021
Published on: 30.06.2021
doi: https://doi.org/10.52688/ASP90525

Decoding of convolutional codes using viterbi algorithm

Dhamyaa Salim mutar [1,*]

[1] Baghdad College of Economic Sciences, Baghdad, Iraq

[*]dhamyaa.salim@baghdadcollege.edu.iq

ABSTRACT

The development of computer applications and widely emerged internet services enforces adaptation of more enhanced means for security. Information encryption is being demanded in order to prevent the autonomous attempts to claim the data. The challenges of information encryption are raised after the internet data inventory were invented as data broadcasting through a public network may be penetrated by unauthorized receivers. This paper is presenting the Viterbi algorithm that is manifested a robust solution for convolutional codes decoding. Two designs are being discussed namely convolutional coding with 1:2 and 2:4 code rates.

Keywords: Convolutional codes, encoding, decoding, code rates, source coding, MSB, LSB

INTRODUCTION

The literature of Information security is backed to 50 B.C. when the Caesar Cipher and others invented a techniques (methods) for tempering detection on the correspondences for protecting the confidential information for the unauthorized claims [8]. This approach is further developed thereafter where coding of signals exchanged amongst sealers is performed by using Morse codes (Figure 1). Morse codes invented after Britain Philips invented a column of lamps that reveal the signals using Morse codes. This technology is used in marine applications and also in other ground applications.

Encryption of information using optical methods (i.e. Mores codes based optical encryption) have made exceptional contribution in information/correspondence security on those days. The advancement of data is motivated more development in the information security means. Coding theories are begun to appear for supporting the large stream of data among the communicated pairs.

In today's life, digital image [5], digital voice [6] also other biometrics such as hand [9], eye [7], etc. are used for data encryption. Voice features are being extracted in both time domain and frequency domain in order to grant access for the authorized person in the so called personal identification system stated at [9]. Similarly, the face features are extracted using digital image processing techniques for evaluating the identity of the person as illustrated at [8].

In more paramount applications such as wireless signal transmission where the signal can be received by endless users, the autonomous attacks are more prone and hence, source coding is being deployed for encryption of transmitted signal at the source. Channel where information is propagating from the source to destination (s) is encountered for uncertain fluctuations i.e. Additive White Gaussian Noise (AWGN) noise that alter the transmitted data and let to autonomous attacks prone.

So to say, channel coding is also invented for the applying security constrains to the signal that is already broadcasted through the said channel. Channel coding is more about increasing the noise immunity of the information signals sent form the transmitter to the receiver through a known channel. However, coding technology must be wrapped with decoding technology so that the received/ authorized one will be equipped with those tools and keys to decode the received data. In this paper, channel coding and decoding approaches are developed with light of convolutional codes and Viterbi decoding algorithm. two types of codes are demonstrated in in order to determine the different code rates design considerations and requirements.

CODING THEOREM

Encryption of information (data) with unique identifiers in order to prevent the authorization claims on those data is termed as coding. It has clearly understood with primitive coding approach on Mores codes (Figure 1).

***Corresponding author**
Dhamyaa Salim mutar,
Baghdad College of Economic Sciences, Baghdad, Iraq
e-mail: dhamyaa.salim@baghdadcollege.edu.iq

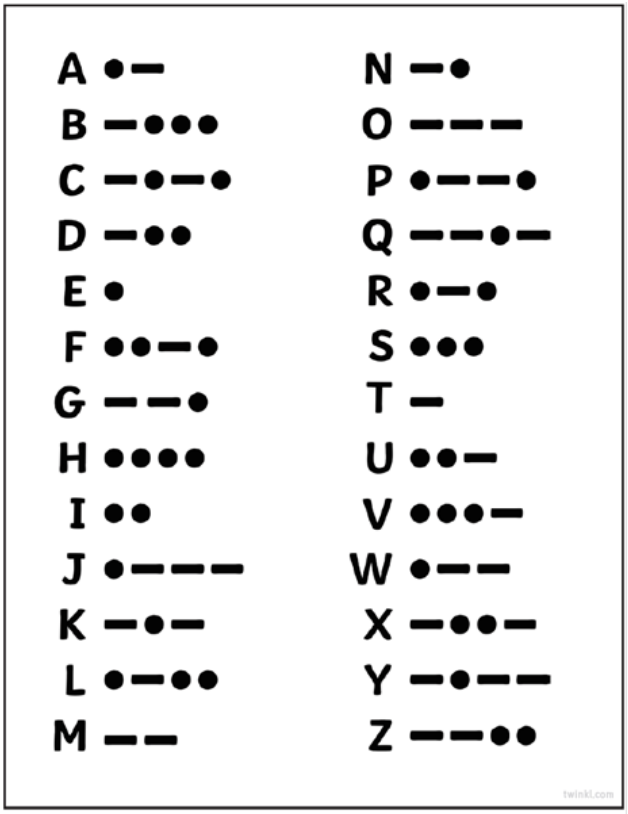

Figure 1: Mores's code legend demonstrates the English alphabetic representation

The advancement of information technology raises the source coding and encryption of data. However, within binary formatted data, the coding is required more than the technology of encryption at Mores codes. Miller code is presented later with capability to perform source coding in order to enhance the data immunity while sending through noisy channels. Miller's code [] is dealing with binary formatted data which converts the digits into encrypted format according to the flowing coding procedure.

(a) coding procedure is basically about inversion of signal digits e.g. zero to one OR one to zero. However, if bits are all zeros then no inversion will be taking place.

(b) now it a bit value is zero and this bit is preceded by other zero bit then signal bits at the edges of this bit is converted (reversed).

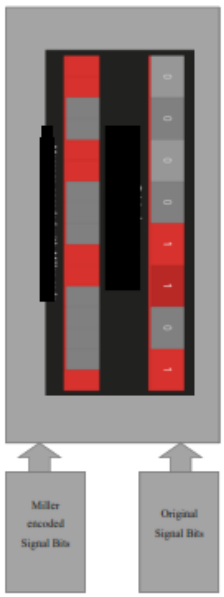

Figure 2: Miller's code legend demonstrates the English alphabetic representation

*Corresponding author
Dhamyaa Salim mutar,
Baghdad College of Economic Sciences, Baghdad, Iraq
e-mail: dhamyaa.salim@baghdadcollege.edu.iq

(c) when bit value is one, the inversion is taking place by inverting the signal located at the middle of this bit. Figure 2 is demonstrating those steps.

Convolutional code involves using shift register (Figure 3) this is representing an electronic registers (gates) in different number (the selection of gate units' number is depending on design requirements, the greater number of shift-register units, the more security enforced). Data bits (binary formatted) is feed into the said shift register from either least significant bit (LSB) direction or from the most significant bit direction (MSB). Electronic devices such as D-Flipflops are subset of the shift register. Each flipflop can be triggered with clock signal so that each input is jumped to the next input flipflop.

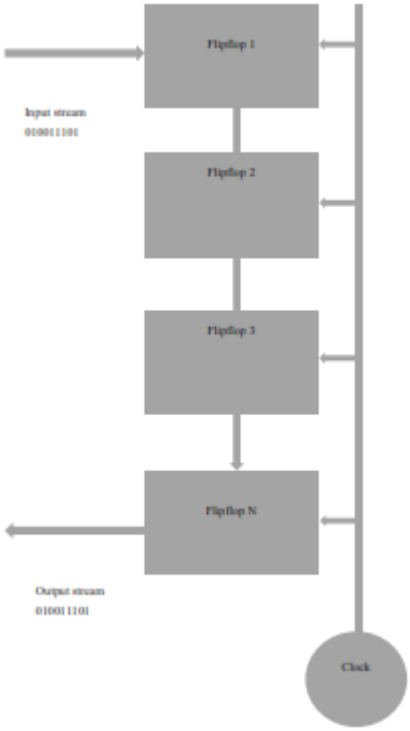

Figure 3: Shift register structural overview, containing of N flipflops

CONVOLUTIONAL ENCODER

The processing of data from the input through the series of flipflops in the shift register is representing the core of convolutional coder. Additional electronic devices such as exclusive OR logic gate is incorporated to this complex in order to form the output coding style (Figure 4).

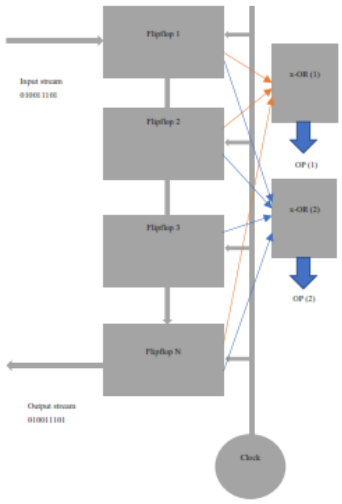

Figure 4: Shift register based convolutional encoder (design 1)

*Corresponding author
Dhamyaa Salim mutar,
Baghdad College of Economic Sciences, Baghdad, Iraq
e-mail: dhamyaa.salim@baghdadcollege.edu.iq

The convolutional coding procedure is taking place firstly by assigning of zeros logic into all gates (flipflops) in the shiftregister. The input signal (bits) of nine bits i.e. 010011101 is applied at the LBS side of the shift-register. Within each trigger of clock in the shift register, the current state (bit) of nth flipflop is shifted into the next flipflop. At every clock cycle, output is detected by x-OR gates.

Figure 5: Shift register based convolutional encoder (design 2)

In out design we proposed the structure of convolutional encoder illustrated in Figure 4 and other one that illustrated in Figure 5. Number of X-OR gate in the first design is two logic gates. The number of X-OR logic hates in the design is representing the code rate, for example for nine bits input message and two x-OR logic gates outputs, with four units of flipflops, the code rate for this encoder is 2/4= 1/2. In the second design, five units of flipflops with three x-OR logic gates are used, the code rate is represented as 3/5. The greater number of shift registers and x-OR logic gates results in enhanced coding security in overall system.

VITERBI ALGORITHM

Viterbi algorithm is outstanding technique for decoding the convolutional codes. It uses multi-state diagram for evaluating the output but from each transaction and however, evaluating the shortest path in the Trellis diagram [8].

Figure 6: State-diagram and Trellis diagram prototype

*Corresponding author
Dhamyaa Salim mutar,
Baghdad College of Economic Sciences, Baghdad, Iraq
e-mail: dhamyaa.salim@baghdadcollege.edu.iq

Figure 7: Trellis diagram where Viterbi algorithm is applied for determining the shortest path

Figure 7 outlines encoder and trellis state chart for 8-state input signal. Owing to the restriction forced by the encoder, there are as it were a constrained set of state moves related with the certain phasor arrangement is as it were conceivable. Presently, the over specified rules will be much clearer with this illustration. For illustration, let the right way be all zero way and what will be the most brief remove between the two paths which diverges and after that remerges, that's given by least squared remove free Euclidian remove of the code.

CONCLUSION

This paper involved design procedures for two prototypes of convolutional encoders; both designs are encountered for the amount of system complexity. That can be judge by the number of output x-OR logic gates inserted to the system (encoder) as well as the number of the flipflops chains inserted into the system. The experiments that conducted in this approach have revealed the flowing points:

(a) The higher rate i.e. greater number of logic gates at the coder output is more robust encoder that the lower one. This is manifested by the number of the output bits as more combinations of the output in front of each input bit is producing more complicated codes that difficult to be penetrated.

(b) Using of Viterbi algorithm for decoding of convolutional codes is prone to computational power as finding the optimum path (distance) is depending on each branch calculation in the Viterbi Trellis diagram.

(c) Convolutional coding is outstanding technology for binary channel coding that create immune coded signal against channel uncertainties such as Additive White Gaussian Noise (AWGN) noise and interferences.

REFERENCES

[1] Zeyad Taha Yaseen,,'Performance Analysis of DPSK Technique for Optical Transmission Systems',Journal of Positive Sciences, Issue:2, Volume(2021), 2021 Page(510).
[2] Zaman Nagy,Mousa K. Wali,'Enhancement of Virtual Private Network Security Using Machine Learning Technologies',Journal of Positive Sciences, Issue:2, Volume(2021), 2021 Page(1-4).
[3] Gaffala Ali Aborisha,Dogu Çagdas ATILLA, Çagatay AYDI,'Domain Specific Modeling Language For Agile Software Development Types',Journal of Positive Sciences, Issue:1, Volume(2021), 2021 Page(25-30).
[4] Demet Irkli Eryildiz,Marim M A Baka,' Solar Energy as Emergency Power Resource, the Design Specifications and Requirements',Journal of Positive Sciences, Issue:1, Volume(2021), 2021 Page(10-17).
[5] Xue Lv, Mingxia Su, Zekun Wang, Application of Face Recognition Method Under Deep Learning Algorithm in Embedded Systems, Microprocessors and Microsystems, 2021.
[6] Neethu Mariam Joy, et al, DNNs for unsupervised extraction of pseudo speaker-normalized features without explicit adaptation data, Speech Communication 92 (2017) 64–76.
[7] Mohammad Azharuddin Laskar, HiLAM-state discriminative multi-task deep neural network in dynamic time warping framework for text-dependent speaker verification, Speech Communication 121 (2020) 29–43 .
[8] Xiaolong Jiang, et al, Crowd Counting and Density Estimation by Trellis Encoder-Decoder Networks, 2019 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR), 2019.
[9] W. Kang, "Palm vein recognition based on multi-sam-pling and feature-level fusion," Neurocomputing, vol.151, 2015

*Corresponding author
Dhamyaa Salim mutar,
Baghdad College of Economic Sciences, Baghdad, Iraq
e-mail: dhamyaa.salim@baghdadcollege.edu.iq