OPEN ACCESS

International
Journal
Of Modern Engineering Research (IJMER)

Secure Communication With Lossless Data Compression Using Dpd Encoding

Er.Aradhana Raju[1], Purabi Mahato[2], Ritto K. Babu[3], Richi Patnaik[4]
[1-2-3-4]*Department of ECE, Silicon Institute of Technology, Bhubaneswar, Khurda (Dist.), Odisha, India – 751024*

ABSTRACT:- *Densely Packed Decimal (DPD) is an refinement of the Chen ho encoding. It gives the same compression and speed advantages but is not limited to multiples of three digits. The DPD encoding allows arbitrary-length decimal numbers to be coded efficiently while keeping decimal digit boundaries accessible. During the last decades, information security has become a major issue. Cryptography plays major roles to the fulfillment of these demands. This paper shows the implementation of the Densely Packed Decimal Encoding, proposed by M. F. Cowlishaw and simulate using available software platforms. Then transmit the compressed data by using secure communication technique.*

Keywords:-*BCD, DPD, Encryption, Decryption.*

I. INTRODUCTION

In communication data transmission occurs in binary form which is based on digital electronics. The most common encoding that is widely used for decimal data is Binary Coded Decimal Encoding (BCD) in which a single decimal digit is represented by four bits.

The Binary Coded Decimal encoding has always dominated decimal arithmetic algorithms and their hardware implementation by virtue of ease of conversion between machine- and human-readable formats, as well as a more precise machine-format representation of decimal quantities.

1.1Data Compression

As compared to typical binary formats, BCD's principal drawbacks are a small increase in the complexity of the circuits needed to implement basic mathematical operations and less efficient usage of storage facilities.BCD does not make optimal use of storage (about 1/6 of the available memory is not used in packed BCD).

Chen and Ho described a scheme for encoding decimal data which is quite efficient. The Chen-Ho encoding, as it is called, compresses three decimal digits into 10 bits with very little waste, giving a 17% more compact encoding than BCD(which uses 12 bits to store three decimal digits).It uses a Huffman code, with most significant bits selecting various digit combinations.

The main advantage of Chen-Ho encoding over binary representation in 10 bits is that only simple Boolean operations are needed for conversion to or from BCD; multiplication and divisions are not required.

Another encoding technique proposed by M. F. Cowlishaw, Densely Packed Decimal (DPD**),** uses an equivalent encoding to the Chen-Ho scheme, but it is an improvement over Chen-Ho encoding and hence has further advantages. The main advantage over Chen-Ho encoding is that it is not restricted to the fact that for compression the decimal digits should be in multiple of three, which is the primary requirement of Chen-Ho encoding.

DPD encoding technique results in efficient decimal arithmetic and makes efficient and optimized use of available resources such as storage or hardware implementation. And thus resulting in lossless data compression.

1.2 Secure Communication

During the last decades, information security has become a major issue. Encrypting and decrypting data have recently been widely investigated and developed because there is a demand for a stronger encryption and decryption which is very hard to crack. Cryptography plays major roles to the fulfillment of these demands. Secure communication is a way to transmit serial binary data with encrypted form. Cryptography is a physical process that scrambles information by rearrangement and substitution of content, making it unreadable to anyone except the person capable of unscrambling it. Unscrambled information called plaintext is to be

transmitted. e.g.:-credit card number, password, bank account etc. A key is used to encrypt and decrypt the plaintext data. Plaintext data is encrypted to form the cipher text and the parallel data converted to serial form which is then transmitted. At the receiver end by using same key we can decrypt the data from cipher text data.

II. DENSELY PACKED DECIMAL ENCODING

Densely packed decimal (DPD) is an efficient method for binary encoding decimal digits.
The traditional system of binary encoding for decimal digits, known as BCD, uses four bits to encode each digit, resulting in significant wastage of binary data bandwidth (since four bits can store 16 states and are being used to store only 10). Densely packed decimal is a more efficient code that packs three digits into ten bits using a scheme that allows compression from, or expansion to, BCD with only two or three gate delays in hardware.

2.1 Conversion From Bcd To Dpd

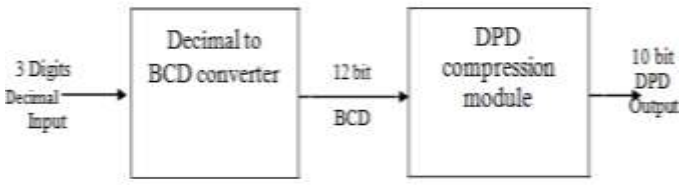
Like Chen–Ho encoding, DPD encoding classifies each decimal digit into one of two ranges, depending on the most significant bit of the binary form: "small" digits have values 0 through 7 (binary 0000–0111), and "large" digits, 8 through 9 (binary 1000–1001). Once it is known or has been indicated that a digit is small, three more bits are still required to specify the value. If a large value has been indicated, only one bit is required to distinguish between the values 8 or 9.When encoding, the most significant bit of each of the three digits to be encoded select one of eight coding patterns for the remaining bits, according to the following table. The table shows how, on decoding, the ten bits of the coded form in columns *b9* through *b0* are copied into the three digits *d2* through *d0*, and the remaining bits are filled in with constant zeros or ones. Bits b7, b4 and b0 (c, f and i) are passed through the encoding unchanged, and do not affect the meaning of the other bits. The remaining seven bits can be considered a seven-bit encoding for three base-5 digits.Bits b8 and b9 are not needed and ignored when decoding DPD groups with three large digits (marked as "x" in the last row of the table above), but are filled with zeros when encoding. The eight decimal values whose digits are all 8s or 9s have four coding each. The bits marked x in the table above are ignored on input, but will always be 0 in computed results. (The 8×3 = 24 non-standard encodings fill in the gap between 10^3=1000 and 2^{10}=1024.)

DPD encoded value										Decimal digits				
b9	b8	b7	b6	b5	b4	b3	b2	b1	b0	d2	d1	d0	Values encoded	Description
a	b	c	d	e	f	0	g	h	i	0abc	0def	0ghi	(0–7) (0–7) (0–7)	Three small digits
a	b	c	d	e	f	1	0	0	i	0abc	0def	100i	(0–7) (0–7) (8–9)	Two small digits, one large
a	b	c	g	h	f	1	0	1	i	0abc	100f	0ghi	(0–7) (8–9) (0–7)	
g	h	c	d	e	f	1	1	0	i	100c	0def	0ghi	(8–9) (0–7) (0–7)	
g	h	c	0	0	f	1	1	1	i	100c	100f	0ghi	(8–9) (8–9) (0–7)	One small digit, two large
d	e	c	0	1	f	1	1	1	i	100c	0def	100i	(8–9) (0–7) (8–9)	
a	b	c	1	0	f	1	1	1	i	0abc	100f	100i	(0–7) (8–9) (8–9)	
x	x	c	1	1	f	1	1	1	i	100c	100f	100i	(8–9) (8–9) (8–9)	Three large digits

2.2 IMPLEMENTATION OF DPD SYSTEM

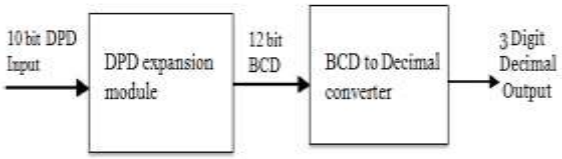
The compression and expansion block of Densely Packed decimal encoding system is designed so as to implement the DPD encoding which is proposed by M. F. Cowlishaw:

COMPRESSION BLOCK



For compression, three digit decimal numbers is passed as input to the compressing block where Decimal to BCD converter converts the binary number in BCD encoded number of 12 bits. This 12 bit BCD number is then fed to DPD compression module which finally compresses the number and encodes it in 10 bits densely packed decimal form.

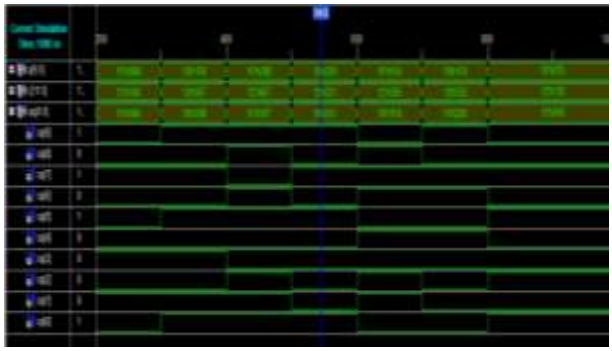
EXPANSION BLOCK



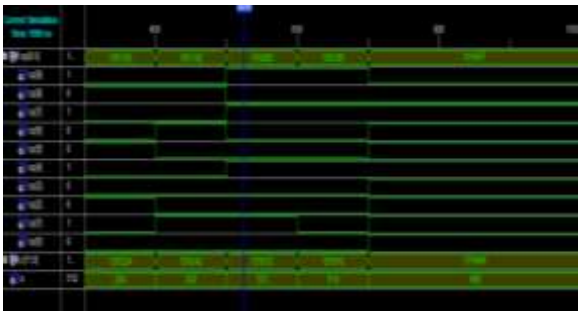
For expansion the 10 bits DPD number is now the input to the expansion block where first it is expanded to BCD form by DPD expansion module. The 12 bits BCD output is then converted to decimal number in simple binary format by BCD to decimal converter.

2.3 Result And Simulation

The following are the simulation results that we got after implementation of the DPD compression and expansion blocks respectively:



Simulation output of Compression Block



Simulation output of Expansion Block

III. SECURE COMMUNICATION AND ITS IMPLEMENTATION

Plaintext - Unscrambled information to be transmitted. It could be a simple text document, a credit card number, a password, a bank account number, or sensitive information such as payroll data, personnel information, or a secret formula being transmitted between organizations.

Cipher text - Represents plain text rendered unintelligible by the application of a mathematical algorithm. Cipher text is the encrypted plain text that is transmitted to the receiver.

Cryptographic Algorithm – Cryptography derived its name from Greek word called "Kryptos" which means "Hidden Secrets".A mathematical formula used to scramble the plain text to yield cipher text. Converting plain text to cipher text using the cryptographic algorithm is called encryption, and converting cipher text back to plain text using the same cryptographic algorithm is called decryption.

Key - A mathematical value, formula, or process that determines how a plaintext message is encrypted or decrypted. The key is the only way to decipher the scrambled information.

Encryption – The process of coding text. The process of disguising a message so as to hide the information it contains; this process can include both encoding and enciphering.

Decryption- The process of decoding text. The decryption process involves converting the encrypted data back to its original form for the receiver's understanding.

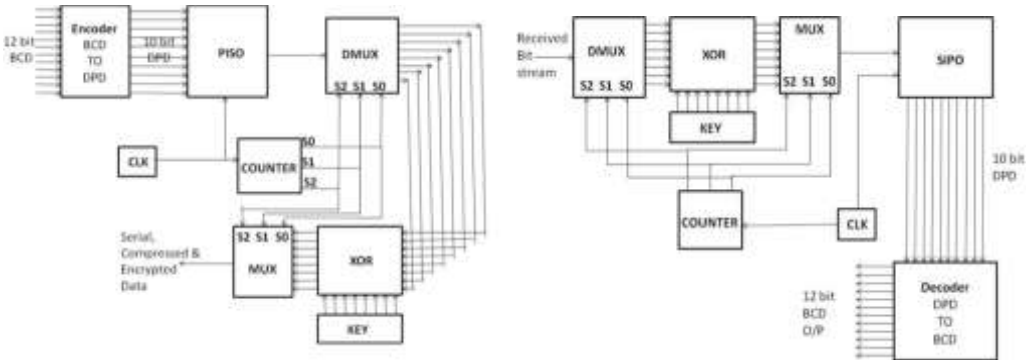
3.1 IMPLEMENTATION OF SECURE COMMUNICATION SYSTEM

3.1.1 Encryption

Data is entered into the DMUX in a linear sequential manner. At select line 000 at the DMUX data is present at the zero'th (0) position of DMUX output. The data is then xored with the key. The select line is provided by the same counter to both the MUX and DMUX. The only thing is that the pulse to the MUX is delivered after a delay of 30ns. And finally we get the cipher text at the output of the MUX.

3.1.2 Decryption

The same thing mentioned above is done in decryption, except that the input here is the cipher text and the output is that plaintext as exact as was input to the encryption system

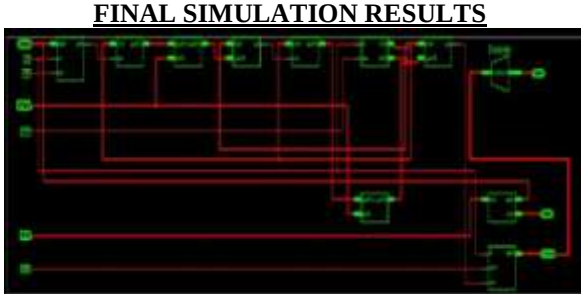


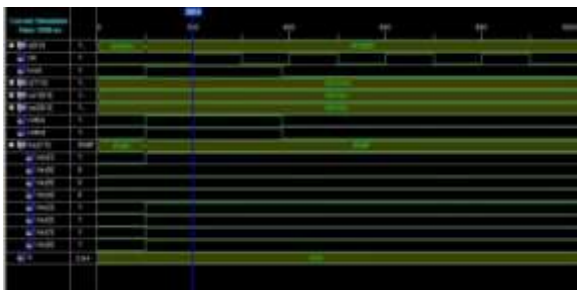
IV. FINAL RESULT AND SIMULATION

Following are the RTL schematic and final simulation results that we have got after encoding the BCD sample into DPD and then converting this plain text into cipher
text using the above explained mechanism (encryption) then transmitting it to the intended receiver where the exact reverse process is carried out (decryption) to obtain the plain text sent.

FINAL RTL SCHEMATIC

FINAL SIMULATION RESULTS





V. CONCLUSION

Here we have implemented DPD logic in VHDL code to compress the data and then transmitted it by using Secure Communication. It has many advantages such as:

1) Reduce disk space required.
2) The log recorders can become shorter.
3) Compressed data can be transferred faster to and from disk.
4) Faster transfer rates across the network.

By applying this coding and communication scheme a larger percentage of hardware complexity can be reduced as well as efficiency can be increased with high degree of security.

Various applications in financial and commercial sector can be optimized by this scheme.

REFERENCES

[1]. S . Rahil Hussian, V. Narasimha Nayak, Dr.Fazal Noorbasha, S. Dayasagar Chowdary, Lakshmi Narayana Thalluri "VLSI Implementation of Densely Packed Decimal Converter to and from Binary Coded Decimal using Reversible Logic Gates"**.** IJERA ISSN: 2248-9622 www.ijera.com Vol. 2, Issue 3, May-Jun 2012, pp. 594-599.

[2]. M.F Cowlishaw, "Densely packed decimal encoding". IEEE Proceedings Computers and Digital Techniques (Institution of Electrical Engineers), 149 (3),pp.102-104,May 2009.

[3]. Kaivani,Alhosseini, A.Z.,Gorgin, S.Fazlali,

[4]. "Reversible Implementation of Densely-Packed-Decimal Converter to and from Binary-Coded-Decimal Format Using in IEEE-754R",Information Technology, 2006. ICIT '06. 9th International Conference on,On page(s): 273-276,Volume:Issue:18-21 Dec. 2006.

[5]. VHDL programming by example 4th edition By Douglas Perry.

[6]. Digital Electronics 4th edition,Morris Mano.

[7]. A Kaivani, A Alhosseini , S Gorgin. and M Fazlali."Reversible Implementation of Densely-Packed-Decimal Converter to and from Binary-Coded-Decimal Format Using in IEEE-754R", pp.273-276, 9th International Conference on Information Technology (ICIT'06), 2009.

[8]. E. Biham, A fast new DES implementation in software, Proceedings of Fast Software Encryption, LNCS 1267, 260-272, Springer 2000.

[9]. [8]M.F Cowlishaw, "Summary of Densely Packed Decimal encoding".

[10]. http://speleotrove.com/decimal/DPDecimal.html

[11]. Binary to BCD converter, http://www,engr.udayton.edu/faculty/jloomis/ece314/notes/devices/binary_to_BCD/bin_to_B CD.html

[12]. Packed decimal encoding IEEE-754-2008 by: J.H.M. Bonten.