IJASRM

International Journal of Advanced Scientific Research and Management, Special issue, CITAES-18

www.ijasrm.com

ISSN 2455-6378

A Survey of VLSI Architectures for Hamming Code Algorithm

Surapaneni Aparna[1], Y. Sri Chakrapani [2], T. Venkata Lakshmi [3] and M. Kamaraju[4]

[1]M.Tech, Embedded Systems, Gudlavalleru Engineering College, Gudlavalleru, India

[2] Associate Professor, ECE Dept, Gudlavalleru Engineering College, Gudlavalleru, India

[3] Associate Professor, ECE Dept,, Gudlavalleru Engineering College, Gudlavalleru, India

[4] Professor, ECE Dept,, Gudlavalleru Engineering College, Gudlavalleru, India

Abstract

In the present innovations, correspondence has numerous applications, and in each field the information is encoded at the transmitter, exchanged over a correspondence channel and got at the recipient after information is decoded. Amid the procedure of transmission in a channel, a few information might be debased because of clamor. At recipient side, blunder information must be distinguished and remedied. Hamming code is one of the famous procedures for mistake discovery and rectification which comprises of encryption and unscrambling process. Encryption is the way toward changing over data or information into a code, particularly headed for counteract unapproved access and Decryption is a procedure of taking encoded or scrambled content and convert it again into unique content. The diverse models of encryption and decoding framework for hamming code calculation are proposed in the writing, which depend on low power, superior, limited expense and so on. In this paper different designs for Encryption, Decryption framework like EC(Encoder)- reversible rationale are indicated and execution qualities are watched dependent on parameters like frame rate, delay are watched for the Hamming code.

Keywords: *Hamming code; Encryption; Decryption; EC-reversible logic;*

1. Introduction

Computerized information transmission is the base of all cutting edge applications. Amid its way from the transmitter headed for collector, mistakes are incited headed for information because of clamor and natural obstruction. A mistake happens when a bit is adjusted among transmitter and recipient. headed for dispose of these blunders, mistake identification and mistake amendment circuits are incorporated with every single advanced circuit. Blunder amendment adds repetition bits headed for the current information headed for make the information transmission impervious headed for outer unsettling influences. Different mistake discovery and adjustment codes are in presence, for example, equality checking, cyclic repetition check, and so on. It adds constrained excess bits headed for the information, keeping the code basic. In any case, Hamming code is a solitary mistake redressing code. It tends headed for be utilized just when the mistake rate is low.

Encryption is the way toward changing data so it is ambiguous headed for anybody yet the proposed beneficiary. Unscrambling is the way toward disentangling scrambled data. A cryptographic calculation, additionally called a figure, is a scientific competence, designed for ascription or else interpretation. Typically, two allied competence have to be exploit, solitary intended for encryption in addition headed for the supplementary meant for decoding. amid mainly here sunlight hours cryptography. The capability headed for go on snarled statistics obscurity are constructed not within illumination of the cryptographic estimate.

What ever be the commonly notorious, conversely lying on a quantity call a solution to facilitate be obliged to subsist utilize amid the estimate headed for deliver an encoded outcome or else headed for denounced recently snarled statistics. sorting out amid the accurate explanation be vital. Decoding lacking the accurate explanation be enormously niggling, if certainly feasible. Hamming code is a solitary mistake amending code. It very well may be utilized just when the mistake rate is low.

2. Error Control Codes

ECC (Error Control Codes) are used to detect and correct the error at the receiver. There are three essential sorts of ECC.

A. Square codes

These codes are alluded headed for while "n" and "k" cipher. A square of k information bits be prearranged headed for end up a square of n bit called a cipher utterance. In square codes, cipher words don't have any reliance on recently encoded messages. NAND Flash memory gadgets normally utilize square codes.

B. Convolution codes

These codes deliver code words that rely upon mutually the in sequence memorandum in addition to a agreed numeral of recently prearranged communication. The encoder change affirm with each message prepared. Ordinarily, the extent of the cipher declaration is consistent.

C. Hamming code

The Hamming code is just the utilization of additional equality bits headed for permitting the recognizable proof of an error [2]. The following is the procedure for Hamming code.

1) Write the bit positions beginning from 1 in twofold frame (1, 10, 11, 100, and so forth).

2) All the bit positions that are an intensity of 2 are set apart as equality bits (1, 2, 4, 8, and so forth).

3) All the other piece positions are set apart as information bits.

4) Each information bit is incorporated into a one of a kind arrangement of equality bits, as decided its bit position in double.

a) Equality bit 1 covers every one of the bits positions whose parallel portrayal incorporates 1 at all huge position (1, 3, 5, 7, 9, 11, and so forth).

b) Equality bit 2 covers every one of the bits positions whose paired portrayal incorporates a 1 in the second position from the minimum noteworthy piece (2, 3, 6, 7, 10, 11, and so on).

c) Equality bit 4 covers every one of the bits positions whose twofold portrayal incorporates a 1 in the third position from the minimum critical piece (4– 7, 12– 15, 20– 23, and so on).

5) Equality bit 8 covers every one of the bits positions whose twofold portrayal incorporates a 1 in the fourth position from the minimum critical piece bits (8– 15, 24– 31, 40– 47, in addition to so on).

6) By and large every equality crumb cover every one of crumbs somewhere the bitwise AND of the egalitarianism spot in addition to the crumb spot be non-zilch.

Since we check for even equality set an equality crumb headed for 1 condition the aggregate digit of ones within the position it check be weird. Situate an equality crumb headed for 0 proviso the aggregate quantity of one's here the position it checks be smooth. A solitary and twofold mistake recognizing coding plan for PC memory frameworks are corrected using new coding strategy The quantity of 1's within the equality prove framework intended for the projected code be less than the entire right now accessible code intended for this reason. The outcomes are improved encoding and unraveling hardware for blunder identification and correction [6].

3. Hamming Code Data Encryption And Decryption System

A. Encryption

It is security apparatus for PC organize. It is procedure of changing over data utilizing a calculation headed for make it unintelligible headed for anybody with the exception of those handling unique information, for the most part alluded headed for as a key. It is the most productive strategy headed for accomplish information security. Encryption can ensure classification of message. For information encryption, a mystery key is utilized. Scrambled information is called as figure message and unscrambled information is called as plain content.

B. Decryption

It is procedure of taking encoded or scrambled content and changing over it once more into unique content. Unscrambling is utilized for un-encoding the information with keys or calculation. Cryptography exploit the extrication procedure next to the hoarder elevation headed for get the earliest memorandum commencing non-comprehensible significance. The decoding route requires two equipment-a Decryption estimate in addition to a enter. A Decryption estimate shows the strategy to facilitate have be utilize in Decryption. Typically, the encryption and decoding calculation are same.

Hamming codes are the most generally utilized direct square codes. Ordinarily, a feint cipher should be characterized as (2n - 1, 2n - n - 1), everywhere as follows:

- n is equivalent headed for the quantity of overhead bits.
- 2n - 1 is equivalent headed for the square size.
- 2n - n - 1 is equivalent headed for comic quantity as concern information chunk during affecting tetragon.

All Hamming codes can recognize three mistakes and one right one. Normal feint cryptogram sizes be

(7, 4), (15, 11), as well as (31, 26). All have a similar feint separation. The feint departures in addition to comic feint burden be valuable in encoding. At the point while the playacting separation is known, the capacity of a cryptogram headed for identify as well as adjust mistakes container survive resolved [3].

A Verilog HDL code is utilized for the feint cipher information encryption and decoding framework, in FPGA [2]. Likewise, the entryway level circuit is planned and executed in CMOS design for three diverse nanometer advances. Fig. 1 demonstrates the square chart of hamming code information encryption and decoding framework.

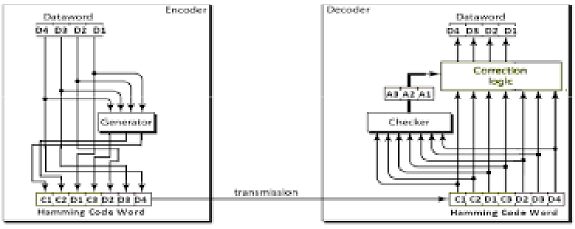

Fig. 1. Block Diagram of Hamming Code Data Encryption and Decryption System

The Hamming cipher canister is utilized in information expressions for several durations. When all is said in done, intended for k prove morsel as well as n information crumb, the aggregate come to of crumb, n + k, to facilitate container subsist during a implicit speech be next to mainly 2k - 1. As it were, the relationship n +k ≤ 2k – 1must hold. This affiliation gives n ≤ 2k – 1 – k as the quantity of bits for the information word [1].

In the (7, 4) expanded Hamming code, the parameters can be pre-registered as:

- Information bits (DI): {DI = D1 D2 D3 D4}
- Code data bits (C): {C = C1 C2 C3}
- Hamming code bits (HC): {HC = HC7 HC6 HC5 HC4 HC3 HC2 HC1}
- Check data bits (A): {A = A1 A2 A3}

The expressions for the (7, 4) expanded Hamming code can be pre-registered as:

$$C1 = D1 \oplus D2 \oplus D4 \qquad (1)$$

$$C2 = D1 \oplus D3 \oplus D4 \qquad (2)$$

$$C3 = D2 \oplus D3 \oplus D4 \qquad (3)$$

$$HC = C1\ C2\ D1\ C3\ D2\ D3\ D4 \qquad (4)$$

$$A1 = C1 \oplus D1 \oplus D2 \oplus D4 \qquad (5)$$

$$A2 = C2 \oplus D1 \oplus D3 \oplus D4 \qquad (6)$$

$$A3 = C3 \oplus D2 \oplus D3 \oplus D4 \qquad (7)$$

In the information transmission side, this framework permits just a 4-bit input information by utilizing this information a 3-crumb rules information bits spirit subsist produced with it spirit included with 4-bit input information, finally 7-smidgen hamming coded information will turn out. This is appeared in the conditions from 1 headed for 5.

TABLE I. Hamming Code Error Detection and Correction - Check Data Bits

Check Data	**Hamming Code Error Bit Logic value Toggling**		
A3 A2 A1	**Data Bit**	**Received Data**	**Corrected Data**
000	No Error	0 1	0 1
001	HC1	0 1	1 0
010	HC2	0 1	1 0
011	HC3	0 1	1 0
100	HC4	0 1	1 0
101	HC5	0 1	1 0
110	HC6	0 1	1 0
111	HC7	0 1	1 0

4. Hamming Code Encoding, Decoding And Correcting Vlsi Architectures

Power upgraded hamming cryptogram indoctrination in addition to disentangling track utilizing referable rationale intended for recognition as well as redress of sole piece mistakes. This thesis planned three referable squares, solitary headed for instruct the current information by including equality bits. The jiffy square creates prove bits. These prove bits help in blunder discovery. here the event that any mistake is acquainted with the cipher remark amid the conduction procedure, the third square recognizes and unravels the prove bits, discovers the defective piece and amends it, accordingly bountiful last blunder free yield. Every one of the above hardware is clarified in the coming areas.

A. *Encryption Architecture*

It is procedure of taking encoded or scrambled content and changing over it again into unique content. Unscrambling is utilized for un-scrambling the information with keys or calculation.

Cryptography utilizes the untying tactic next to the saver plane headed for acquire the initial memorandum commencing non-decipherable communication (symbols transcript). The decoding process requires a two stuff Decryption reckoning. A Decryption calculation demonstrates the method that has been utilized and intended for the mainly element, the encryption in addition to decode reckoning be identical [1].

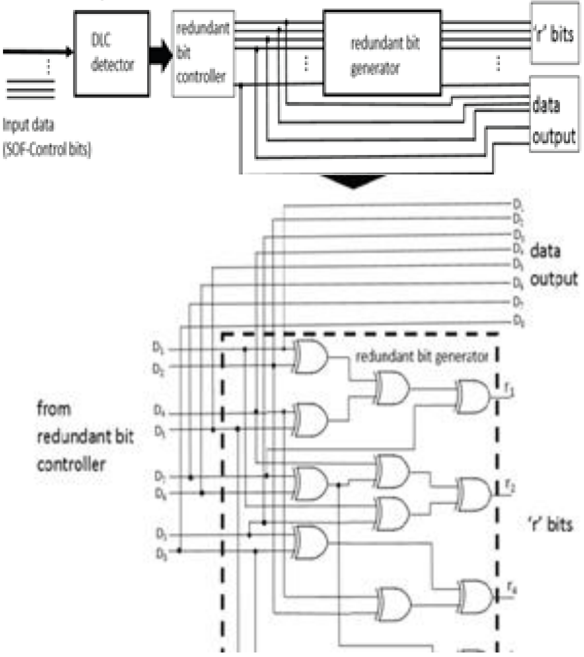

Fig. 2. Hamming Code Encryption Architecture

B. *EC (Encoder) Reversible Logic:*

Cubicle EC be developed utilizing three F2G doors in addition to two FG entryways. EC have stumpy quantum outlay in addition to nought waste yields in this manner improving the supremacy utilization of the track. It have four data sources in addition to seven yields. The four sources of info are information bit. EC cubicle computes equality crumb intended for the agreed information. The equality crumb be set within the spots to facilitate be number within services of 2. The equality morsel be ascertained utilizing the calculation. The yield of FG and F2G doors is just XOR activity of the given sources of info. The yield is 7-tad regulations statement through four in sequence crumb as well as three equality bits. The yield of this chamber be prearranged headed for CG. The engineering of EC be prearranged less.[4]

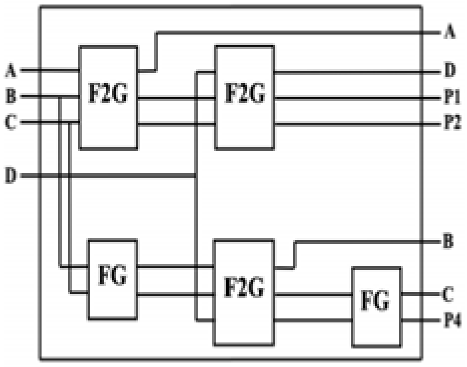

Fig. 3. EC Logic cell architecture

5. Performance Characteristics

In [1], the frame rate examination utilizing CRC codes Vs hamming code when combined and dissected is shown below in Table II. As the number of data frames is increasing, the frame rate for Hamming code is more than CRC.

TABLE II. Frame Rate Comparison using CRC Code Vs Hamming Code

Data Frame (bytes)	**Frame rate (Frame per second)**	
	CRC	Hamming Code
1	2,080.33	2,450.98
2	1,785.71	2,049.18
3	1,582.28	1,785.71
4	1,404.49	1,562.50
5	1,275.51	1,388.89
6	1,157.41	1,250.00
7	1,059.32	1,136.36
8	984.25	1,050.42

Table III shows the delay occurred for data bits and corresponding Hamming code bits when implementing the architecture of encryption and decryption system. When the number of data bits and corresponding Hamming code bits are increased, delay also increases [2].

TABLE.III Delay for Data bits and corresponding Hamming Code Bits

S. No	Data Bits	Hamming Code Bits	Delay(ns)
1	1	1	5.643
2	1	4	6.271
3	1	6	6.179
4	2	2	5.551
5	2	4	6.649
6	2	7	6.165
7	3	3	5.604
8	3	4	6.409
9	3	6	6.32
10	3	7	6.17
11	4	5	5.611
12	4	6	6.196
13	4	7	6.315

6. Conclusions

The Hamming code is the type of error correction code which is utilizes additional equality bits for permitting the recognizable proof of an error. The implementation of VLSI architecture for encryption and decryption system like EC-reversible logic are specified and performance characteristics are observed based on parameters like frame rate, delay. The Hamming code takes the advantage of frame rate over CRC.

References

[1] Ro..Serfa juan, and H.S. kim, and min Woo Jeong , and HyeongWooCha, "FPGA Lmplementation of Hamming Code for Increasing the frame Rate of CAN Communication" IEEE Transactions on Smart Processing and Computing, vol.5, no. 1,pp 29-34, February 2016.

[2] Fazal Noorbasha et al Int, "VLSI Implementation of Encryption and Decryption System Using Hamming Code Algorithm", Journal of Engineering Research and Applications www.ijera.com ISSN : 2248-9622, Vol. 4, Issue 4(Version 1), April 2014, pp.52-55

[3] R. I. Abdul Rahman, and M. B. Tayel, "Simulation of Hamming Coding and Decoding for Microcontroller Radiation Hardening," International Journal of Electrical, Computer, Energetic, Electronics and Communication Engineering, vol. 9, no. 2, 2015.

[4] V. Shiva Prasad Nayak, Govind Prasad, K. Dedeepya Chowdary and K. Manjunatha Chari, "Design of Compact and Low Power Reversible Comparator", 2015 International Conference on Control, Instrumentation, Communication and Computational Technologies (ICCICCT-2015).

[5] R. W. Hamming, "Error detecting and error correcting code," Bell System Technical Journal, vol. 26, pp. 147–160, Apr.1950

[6] P. K. Lala, P. Thenappan, and M. T. Anwar, "Single error correcting and double error detecting coding scheme," IET Electronics Letters, vol. 41, Issue 13, pp. 758–760, Feb. 2005.

[7] Rick Ma and Samuel Cheng "The Universality of Generalized Hamming Code for Multiple Sources", IEEE Transactions on Communications, VOL. 59, NO. 10, PP. 2641- 2647, OCTOBER 2011.

[8] P. Koopman, "32-bit Cyclic Redundancy Codes for Internet Applications," Proc. IEEE International Conference on Dependable Systems and Networks, 2002.

[9] U. K. Kumar, and B.S. Umashankar, "Improved Hamming Code for Error Detection and Correction," in Proc. IEEE, 2nd International Symposium on Wireless Pervasive Computing Conference, pp. 498-500,2007.978