Analysis of VLSI architecture in computerized information transmission using hamming code algorithm

Aasheesh Shukla¹, Manish Kumar²
¹,²Department of Electronics and Communication, GLA University, Mathura
aasheesh.shukla@glau.ac.in, manish.kumar@glau.ac.in

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 clamour. 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.

Whatever 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 affirms 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).
2) 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).

By and large every equality crumb covers 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 ones 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 unravelling 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 estimates 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 2 \((7, 4)\), \((15, 11)\), 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.

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 \(n + k \leq 2k - 1\) must hold. This affiliation gives \(n \leq 2k - 1 - k\) 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:

1) \(C1 = D1 \oplus D2 \oplus D4\)
2) \(C2 = D1 \oplus D3 \oplus D4\)
3) \(C3 = D2 \oplus D3 \oplus D4\)
4) \(HC=C1C2D1C3D2D3D4\)
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 its 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.

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].

![Diagram of Hamming Code Encryption Architecture](image)

**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 has 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.

![EC Logic cell architecture](image)

**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>
<thead>
<tr>
<th>Data Frame (bytes)</th>
<th>Frame rate (Frame per second)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>CRC</td>
</tr>
<tr>
<td>1</td>
<td>2,080.33</td>
</tr>
<tr>
<td>2</td>
<td>1,785.71</td>
</tr>
<tr>
<td>3</td>
<td>1,582.28</td>
</tr>
<tr>
<td>4</td>
<td>1,404.49</td>
</tr>
<tr>
<td>5</td>
<td>1,275.51</td>
</tr>
<tr>
<td>6</td>
<td>1,157.41</td>
</tr>
<tr>
<td>7</td>
<td>1,059.32</td>
</tr>
<tr>
<td>8</td>
<td>984.25</td>
</tr>
</tbody>
</table>

TABLE II. Frame Rate Comparison using CRC Code Vs Hamming Code
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>
<thead>
<tr>
<th>S. No</th>
<th>Data Bits</th>
<th>Hamming Code Bits</th>
<th>Delay(ns)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td>5.643</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>4</td>
<td>6.271</td>
</tr>
<tr>
<td>3</td>
<td>1</td>
<td>6</td>
<td>6.179</td>
</tr>
<tr>
<td>4</td>
<td>2</td>
<td>2</td>
<td>5.551</td>
</tr>
<tr>
<td>5</td>
<td>2</td>
<td>4</td>
<td>6.649</td>
</tr>
<tr>
<td>6</td>
<td>2</td>
<td>7</td>
<td>6.165</td>
</tr>
<tr>
<td>7</td>
<td>3</td>
<td>3</td>
<td>5.604</td>
</tr>
<tr>
<td>8</td>
<td>3</td>
<td>4</td>
<td>6.409</td>
</tr>
<tr>
<td>9</td>
<td>3</td>
<td>6</td>
<td>6.32</td>
</tr>
<tr>
<td>10</td>
<td>3</td>
<td>7</td>
<td>6.17</td>
</tr>
<tr>
<td>11</td>
<td>4</td>
<td>5</td>
<td>5.611</td>
</tr>
<tr>
<td>12</td>
<td>4</td>
<td>6</td>
<td>6.196</td>
</tr>
<tr>
<td>13</td>
<td>4</td>
<td>7</td>
<td>6.315</td>
</tr>
</tbody>
</table>

6. Conclusions

The Hamming code is the type of error correction code which 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


