Abstract

Objectives: This paper proposes efficient extended hamming codes to find & rectify a single error (SEC) as well as find large number of double & triple adjacent errors (DAED) or (TAED). Methods: (n, k) hamming codes are utilized to implement the proposed system. The codeword of (n, k) hamming codes have ‘n’ bit. From these ‘n’ bit error combinations are found by using MATLAB design tool. From detected error combinations, the order of code bits is changed according to bit replacement algorithm. Calculated codewords are shuffled in order to obtain high probability of detection in double & triple errors. Findings: Calculated Hamming SEC-DAED-TAED codes (Bit-reordered codeword) gives 45% of probability of detection improvements in double adjacent error detection and 33% of probability of detection improvements in triple adjacent error detections when compared to normal order based hamming SEC-DAED-TAED codes. 128-bit Advanced Encryption Standard (AES) encryption standard is considered as one of the applications of developed hamming code. Applications: Mobile banking, Internet banking, space and terrestrial communications are considered as the important applications of proposed hamming codes based AES encryption.

Keywords: Advanced Encryption Standard (AES), Bit Replacement Algorithm, Extended Hamming Codes, Error Detection and Correction codes, Very Large Scale Integration (VLSI)

1. Introduction

Hamming Codes are one of the EDC codes which are used to protect the registers and memories from soft errors. As technology scales, radiation particles can create more soft error likely to affect the more than one bit binary number. This type of effects is named as Multiple Cell Upset (MCU). Interleaving is one of key results for overcoming the MCU effect. But, unfortunately, interleaving process would not provide the best solution for the MCU problem. Also, it increases the complexity of device and is not suitable for memory based transmission. On the other hand, hamming code is also can correct single error per word. Hence, it requires the best solution for reducing the MCU effects in data transmission. In order to meet the above requirements, “Extended Hamming Codes” are proposed in this research work.

2. Hamming Code

Hamming codes are used for preventing data corruption while transmitting information over noisy channels. Hamming codes have two problems, increasing the distance and code rate. Several encoding schemes that have dramatic improvements over existing codes are proposed.

For an integer \( z \geq 3 \),

\[
    x = 2^z - 1 \quad (1)
\]

\[
    k = x - z \quad (2)
\]
Extended Hamming SEC-DAED-TAED based Fault Detection Technique for AES Encryption and Decryption

\[ d_{\text{min}} = 3 \]  
(3)

Where \( x \) is the block size, \( k \) is the number of data bits, \( d_{\text{min}} \) is the least distance of the code and \( z \) is the parity check bits.

The shortened lexicographic matrix is shown in equation (4),

\[
H = \begin{pmatrix}
0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\
0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\
0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\
1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0
\end{pmatrix}
\]  
(4)

3. AES Algorithm

The symmetric encryption algorithm use same keys both at the sending and receiving end. AES Algorithm belongs to the symmetric keys encryption method.

The block diagram of 128 bit AES encryption and decryption is shown in Figure 1.

3.1 Sub-Bytes Transformation ()

The techniques use the help of substitution tables. There are two transformation techniques.

1. Multiplicate Inverse (MI) Transformation: The input state bytes on Galois Field GF (2^8) are transformed using multiplicative inverse function.

2. Affine Transformation (AT): In this operation, XOR functions are performed. The transformation permits inverse operation.

\[ \text{Figure 1. Block Diagram for 128 bit AES (a) Encryption (b) Decryption.} \]

3.2 Shift Rows Transformation ()

The transformation for a matrix is shown below,

\[
\begin{bmatrix}
s_0 & s_4 & s_8 & s_{12} \\
s_1 & s_5 & s_9 & s_{13} \\
s_2 & s_6 & s_{10} & s_{14} \\
s_3 & s_7 & s_{11} & s_{15}
\end{bmatrix}
\]

3.3 Mix Column Transformation ()

The columns are interchanged on the basis of key polynomials.

3.4 Add Round Key Transformation ()

Bits are appended in this transformation.

4. Proposed SEC-DAED-TAED Hamming Codes

Hamming code for single bit error correction, double adjacent error detection and triple adjacent error proposed in this work. All permutations of double and triple adjacent errors are detected. Replacement method is used for designing the single error correction, double adjacent error detection and triple adjacent error detection hamming codes. The strategy is shown in Figure 2.

In extended single error correction, double adjacent error detection and triple adjacent error detection hamming code, 6 number of Triple-Adjacent Error and 5 number of Double-Adjacent Error have been detected successfully. There are eleven number of double adjacent error combination and nine number of triple adjacent error combination in 12 bits. Table 1 shows the proposed probability of detection of hamming code.

\[ \text{Figure 2. Flow chart of Bit Re-placement Strategy.} \]
Table 1. Probability of Detection of Hamming Code(12,8)

| Bit Placement | Double Adjacent Error Detection | Triple Adjacent Error Detection |
|---------------|---------------------------------|---------------------------------|
| 1 2 3 4 5 6 7 8 9 10 11 12 | 2/11 18% | 3/9 33% |
| 7 11 6 4 2 9 10 8 1 5 3 12 | 5/11 45% | 6/9 66% |

Proposed Double Adjacent Error Detection and Triple Adjacent Error Detection method detects errors with 45% and 66% probability respectively. Proposed model offers 27% improves the detecting probability of double adjacent error and 33% improves the detecting the probability of triple adjacent error. The proposed method is integrated into Encryption and Decryption Process. Proposed Block diagram of Encryption and Decryption structure by using the proposed work has been illustrated in Figure 3. Further Table II illustrates the groups for bit error detection.

5. Results and Discussions

Hamming Code shows the status indication when correcting SEC or detecting DAED and TAED. Simulation result of Encryption and Decryption is illustrated in Figure 4. Figure 5 illustrates the Single Error Correction (SEC) while data communication in AES Encryption and AES Decryption. Similarly Figure 6 and Figure 7 illustrate the status while data communication in Encryption and Decryption.

Encryption using the method proposed has been illustrated in Figure 8. Similarly, Decryption using the method proposed has been illustrated in Figure 9.

Plain Data

| AES Encryption | Plain Data |
|----------------|------------|
| Extended Hamming | AES Decryption |
| SEC-DAED-TAED Encryption | Extended Hamming SEC-DAED-TAED Decryption |

Cipher Data

Figure 3. Architecture of described Encryption and Decryption.

Table 2. Groups for Bit Error Detection

| Traditional Hamming Code Number System | Proposed Extended Hamming SEC-DAED-TAED Number System |
|---------------------------------------|------------------------------------------------------|
| Double Adjacent Error | Triple Adjacent Error | Double Adjacent Error | Triple Adjacent Error |
| (4, 5) | (3, 4, 5) | (7, 11) | (6, 7, 11) |
| (7, 8) | (1, 2, 3) | (2, 4) | (4, 6, 11) |
| (8, 9, 10) | (8, 10) | (8, 10) | (2, 4, 6) |
| (1, 5) | (1, 5) | (8, 9, 10) | (2, 4, 9) |
| (3, 12) | (3, 12) | (2, 9, 10) | (2, 9, 10) |

Figure 4. Encrypted Data Transmission and Reception.
6. Conclusion

The disadvantages of conventional hamming codes are Silent Data Corruption (SDC). This is totally eliminated in the code. Proposed codes offers forty five percent two bit, and sixty six percent three bit correction whereas conventional method offers eighteen percent two bit, and thirty three percent three bit ability. Hence, it offers 27% of enhanced DAED probability and 33% of enhanced TAED than conventional one. Further the integrated method will be suitable for all encryption and decryption applications.

7. References

1. Ahmad N, Hasan SR. Low-power compact composite field AES S-Box/Inv S-Box design in 65nm CMOS using Novel XOR Gate. Integration. The VLSI Journal. 2013; 46(4):333–44.
2. Antony B. Modified Hamming Codes with Double Adjacent Error Correction along with Enhanced Adjacent Error Detection. International Journal of Innovative Research in Computer and Communication Engineering (IJJRCCE). 2015; 3(8):7706–13.
3. Balamurugan J, Logashanmugam E. Design of High Speed and Area Efficient Optimized MixColumn for AES. International Journal of Applied Engineering Research (IJAER). 2015; 10(17):13003–8.
4. Chandrika S, Rani Hema Malini R. Efficient Implementation of Hamming SEC-TAED Code Algorithm for Data Communication. International Journal Innovative Research and Studies (IJIRS). 2014; 3(11):276–89.
5. Cui Y, Lou M, Xiao J, Zhang X, Shi S, Lu P. Research and implementation of SEC-DED Hamming code algorithm. In TENCON 2013-2013 IEEE Region 10 Conference (31194) (pp. 1-5). IEEE.4. D.L. Eaton, Porous Glass Support Material, US Patent No. 3 904 422.
6. Sanchez-Macian A, Reviriego P, Maestro JA. Enhanced detection of double and triple adjacent errors in hamming codes through selective bit placement. IEEE Transactions on Device and Materials Reliability. 2012; 12(2):357–62.
7. Sanchez-Macian A, Reviriego P, Maestro JA. Hamming SEC-DAED and extended hamming SEC-DED-TAED codes through selective shortening and bit placement. IEEE Transactions on Device and Materials. 2014; 14(1):574–6.
8. Satyanarayan NV, Sujatha NL, Ramaraju JSS. Detecting and Correcting Multiple Upsets with 64-bit Decimal Matrix Code in Memories, International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering (IJAREEIE). 2014; 3(8):11496–504.
9. Baek S-S, Won Y-S, Han D-G, Ryou J-C. The Effect of Eight-Shuffling AES Implementations Techniques against Side Channel Analysis. 2015 Mar; 8(5):91–7.
10. Vignesh B. Pipelined Quadratic Equation Based Novel Multiplication Method for Cryptographic applications. 2014; 7(4):34–9.