Efficient Fault Detection Model Design “Hamming SEC-DAED-TAED-TETRA AED” Based AES Encryption and Decryption

M. Vaidehi  
Research scholar, Karpagam University, Coimbatore, Tamilnadu, India.

Dr. B. Justus Rabi  
Principal, Shri Andal Alagar College of Engineering, Chennai, Tamilnadu, India.

Abstract  
The high level of security and the fast hardware and software implementation of the Advanced Standard Encryption (AES) have made it in the first choice for many critical applications. Advanced Encryption Standard (AES) is the self-determining hardware architecture for producing crypto mechanism. In a secure transmission system, Content Addressable Memory (CAM) based transmissions always provide Silent Data Corruption (SDC). In order to overcome this problem, Extended hamming code has been executed in this paper for reducing the SDC effect in AES Encryption and Decryption. In the fault detection and correction mechanism, Single Error Correction based hamming codes are available. Single Error Correction (SEC) and Double Adjacent Error Detection (DAED) are done by using hamming codes. In order to detect triple adjacent error in SEC-TAED, it is required to add one parity bit, which consumes more amount of computational time for detecting the triple adjacent error. SEC-Tetra AED is also required to add one more parity bit for detecting for detecting the tetra adjacent error. To overcome this problem, Hamming codes are extended in this paper for making a new faulty detection system. In the proposed Faulty detecting system referred as Extended hamming single Error Correction-Triple Adjacent Error Detection-Tetra Adjacent Error Detection (SEC-DAED-TAED-Tetra AED) method. Further proposed Extended Hamming SEC-DAED-TAED-TetraAED error correction codes are incorporated into 128-bit AES Encryption and Decryption for increasing the crypto properties and also reducing the complexity of S-box and mixed column in AES. Implementation of Proposed Extended Hamming SEC-DAED-TAED-Tetra AED based AES encryption and decryption has been done through Very Large Scale Integration (VLSI) system design environment. Error Correcting Codes are ubiquitous. They are adopted in almost every modern digital communication and storage system in a application such as wireless communications, optical communications and flash memories, computer hard drives, sensor networks and deep-space probing. New-generation and emerging applications demand codes with better error-correcting capability.

Keywords: Advanced Encryption Standard (AES), Silent Data Corruption (SDC), Content Addressable Memory (CAM), Single Error Correction (SEC), Double Adjacent Error Detection (DAED), Triple Adjacent Error Detection (TAED), Tetra Adjacent Error Detection (Tetra AED).

Introduction  
Hamming codes are introduced more than 60 years ago and they are still used in many applications. Hamming codes are widely used to detect and correct an error during the data transmission. Hamming codes were presented that can correct one error per word are widely used to protect the soft errors which occur when a radiation particle hits the device and changes the logical values. The encoding and decoding latency for hamming directly affect the memory access time. Single Error Correction (SEC) codes have a minimum hamming distance of three and therefore double error can be mistaken for a single error erroneously corrected. SEC-DAED codes have a minimum hamming distance four. A SEC-DAED code can be created by extending a hamming code with a parity bit covering all bits. The additional parity bit is easily generated as the combination of all bits and checked by comparing it to the parity of the code word excluding the bit itself. This process can be done independently or matrices can be modified. All the triple adjacent errors are detected due to the special configuration of the check matrix, except the one affecting the additional parity bit and its two adjacent code word bits.

The AES is a symmetric key block encryption algorithm. The symmetric key algorithms are algorithms that use the same key to perform an operation and its inverse. Advanced Encryption Standard (AES) is the data security principle which used to exhibit the secure transmission between the sender and receiver. In AES algorithm, four types of transmissions are used to provide the cipher data from plain data such as S-Box (Substitution Box), Shift Rows, MixColumn and Add Round Key. Like that, four reverse transformations are also used in AES decryption algorithm to recover the plain data from cipher data such as Inverse S-Box, Inverse Shift Rows, Inverse MixColumn and Add Round Key. In this research work, fault detection and correction system has been designed along with data security principle. Fault detection system is based on Extended hamming codes can be extended by adding one or more parity bit with traditional one. Proposed extended hamming codes can correct a single error and can detect the more possibilities of double, triple and tetra adjacent bit error in data transmission. Therefore, the Proposed Fault detection system named as “Hamming Single Error Correction-Triple Adjacent Error Detection and Tetra Adjacent Error Detection (SEC-DAED-TAED-Tetra AED) codes. Further proposed Extended Hamming SEC-DAED-TAED-TetraAED codes have been incorporated into AES Encryption and AES.
decryption algorithm for increasing the accuracy and security of the data transmission.

Related Works
Enhanced Detection of Double and Triple Adjacent Errors in Hamming Codes Through Selective Bit Placement has been explained in [Sanchez-Macian, et al, 2012]. In this paper, hamming codes are used to increase the probability of detecting double and triple adjacent errors. The enhanced detection is achieved by placing the bits of the word such that adjacent errors result in a syndrome does not match that of any single error. Low-Power Compact Composite Field AES S-Box/Inv S-Box design in 65nm CMOS using Novel XOR Gate has been described in [Ahmad, N, et al, 2013]. This paper presents a full custom CMOS design of S-Box/Inv S-Box with low power GF (2^n) Galois Field Inversions based on polynomial basis, using composite field arithmetic. In 65 nm IBM CMOS technology, the S-Box/Inv S-Box utilizes a novel low power 2-input XOR gate with only six devices to achieve a compact module implemented. This design indicates a power dissipation of only around 0.09µW using a 0.8V supply voltage.

On Forward Error Correction with Hamming Code for Multi-path Communications have been explained in [3]. In this paper, the performance bound in the high error-rate networks and integrated multi-path communication and Hamming code (11-7). The performance of Multi-path Hamming Code based Forward Error Correction (FEC) is analyzed and compared with Multi-Path Power Control (MPC), by using the Markov model. Bit-Level Soft-Decision Decoding of Double and Triple-Parity Reed-Solomon Codes Through Binary Hamming Code Constraints has been described in [4]. This paper discussed bit-level soft-decision decoding of double and triple-parity Reed-Solomon (RS) codes through binary Hamming Code constraints. Based on the binary image of RS code, they first present the new expressions of the associated parity-check equations. These expressions indicate that each parity-check equation of RS code with roots αi (0 < i < 3) over GF (2^4) can be viewed as parity-check equations of a compound Hamming code over GF (2).

Hamming Code
Hamming code is a set of error-correction codes that can be used to detect and correct bit errors that can occur when computer data is moved or stored. Hamming codes are invented by Richard Hamming in 1950, which is a family of linear error correcting codes that generalize the hamming codes. Without any detection of uncorrected errors, Hamming codes can detect up to two bit errors or correct one bit errors. Hamming codes are perfect codes, that is, they achieve the highest possible rate for codes with their block length and minimum distance of three. In mathematical terms, Hamming codes are denoted by the following parameters, For an integer m≥3,

\[
\begin{align*}
&n = 2^m - 1 \quad (1) \\
&k = n - m \quad (2) \\
&d_{	ext{min}} = 3 \quad (3)
\end{align*}
\]

Where n is the block size, k is the number of information bits, d_{\text{min}} is the minimum distance of the code and m is the parity check bits. For a single error correction, the minimum number of hamming distance is three that means three parity bits are used to detect and correct single bit error.

The general algorithms for generating SEC hamming codes are as follows:

1) Number the bits starting from 1: bit 1, 2, 3, 4, 5, etc. 2) Write the bit numbers in binary : 1, 10, 11, 100, 101, etc. 3) All bit positions that are powers of two (have only one 1 bit in the binary form of their position) are parity bits: 1, 2, 4, 8, etc. 4) All other bit positions, with two or more 1 bits in the binary form of their position, are data bits. 5) Each data bit is included in a unique set of 2 or more parity bits, as determined by the binary form of its bit position.

Step 1: To verify 1 bit and bound 1 bit steps are followed such as 1, 3, 5, 7, 9, ….

Step 2: To verify 2 bits and bound 2 bits steps are followed such as 2, 3, 6, 7, 10, 11, ….

Step 3: To verify 4 bits and bound 4 bits steps are followed such as 4, 5, 6, 7, 12, 13, 14, 15, …

Step 4: To verify 8 bits and bound 8 bits steps are followed such as 8-15, 24-31, 40-47, …

In hamming code, the decoder can detect and correct a single error and at the same time detect the double error but not correct that error. In order to avoid this problem, the extended versions of hamming code used, there is a additional parity is used to detect the double error. Inappropriately, the algorithm can be used for detect the triple adjacent error and Tetra adjacent error.

Two techniques are used to detect the double bit error, one is the bit replacement or reordering the codeword, when lexicographic matrix is used for detecting and correcting a single error and another one is shortening technique. The
shortened hamming code (12,8) of lexicographic matrix is shown in equation (4)

\[
H = \begin{bmatrix}
0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \\
0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 \\
0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\
1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 
\end{bmatrix}
\]

(4)

When a single bit error occurs in the code word, the syndrome vector that results from the product of the lexicographic matrix with the error code word gives the binary representation of the position where the error was inserted. For example, hamming code (12, 8), data bits (0101010100) are coded as (0000101111010). When an error occurs and, for instance, the fifth bit is changed the code word turns into (00001110100). The product of this vector by lexicographic check matrix results in the syndrome vector (1010) corresponding to the binary representation is five and therefore we can easily detect and correct the error. Coming next to the previous example, if there is a double bit error in original word in position 5 and 6, we get the vector (000001110100). Now the product of this vector by lexicographic check matrix results in the syndrome vector is (0011) corresponding to binary representation is 3. In this case, codeword is in corrected instead of correcting right word.

**AES ALGORITHM**

The Advanced Encryption Standard or AES is a symmetric block cipher used by the U.S. government to protect classified information and is implemented in software and hardware throughout the world to encrypt sensitive data. **Advanced Encryption Standard (AES)** is a symmetric encryption algorithm. The algorithm was developed by two Belgian cryptographers Joan Daemen and Vincent Rijmen. AES was designed to be efficient in both hardware and software, and supports a block length of 128 bits and key lengths of 128, 192, and 256 bits. AES algorithm consists of two parts, one part is data procedure and another part is Key schedule. The data procedure is the main body of the encryption (decryption) and consists of four operations, (Inv) sub bytes, (Inv) Mix column, and (Inv) Add Round Key.

The General data flow structure for 128 bit AES Encryption and Decryption is illustrated in fig.1. As shown in fig. 1, Final round of both AES Encryption and AES Decryption doesn’t have Mix Column and Inv Mix Column transformation function respectively. It has 10 numbers of rounds for exhibiting cipher data from encryption process and plan data from decryption process.

**SUB-BYTES TRANSFORMATION ()**: Substitution techniques are involved with the help of substitution tables (LUTs/ Memories/ ROM), in Sub-Bytes transformation. In substitution box have a two transformation techniques, they are

1. Multiplytive Inverse (MI) Transformation: To perform multiplicative inverse function for given input state bytes on Galois Field GF (2^8).

2. Affine Transformation (AT): To perform Affine Transformation of MI outputs. In this operation, XOR functions can be performed with in combined input bits itself. Similarly, Inverse Sub-Bytes transformation performs inverse operation.

**SHIFT ROWS TRANSFORMATION ()**: In Shift Rows operation, only changes the byte position in the state.

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

The first row is not changed, the second row is left shifted by one, the third row is by two and the last row is by three. Similarly, reverse process has been followed in Inv shift Rows Transformation.

**MIX COLUMN TRANSFORMATION ()**: The state bytes are treated as a Four-term polynomial in the mix column transformation. Then the columns are considered as polynomials over GF (2^8) and multiplied modulo x^4 + 1 with fixed polynomials. Similarly, the reverse process has been followed in Inv Mix Column Transformation.

**ADD ROUND KEY TRANSFORMATION ()**: A round key is added to the state by a simple bitwise XOR operation, in add round key transformation. Each round key consists of N_b words. Those N_b words are added into the columns of the state.
Proposed SEC-DAED-TAED-TETRA AED HAMMING Codes

In this research work, Selective bit placement based algorithm has been developed to improve the detection probability of error bit while transferring the data between two nodes or networks. In previous works, detection of three adjacent bit errors is studied. However, possibilities of occurring three bit errors are very less, because in every data communication process, information’s are transformed in terms of bytes (even number of bits). Hence, it is essential to maximize detection probability of Tetra Error. In order to fulfill the above requirement, hamming codes of previous work has been extended in this paper. A proposed new hamming code is called as “Extended Hamming SEC-DAED-TAED-Tetra AED”. Proposed hamming code can detect & correct a single error and can able to detect the double, triple and tetra adjacent error. In order to maximize the detection probability of tetra adjacent error detection, bit placement rules has been used on the codeword of encoding part. Table I shows the new codeword format for SEC-DAED-TAED-Tetra AED.

![Figure 2: Flow chart of Bit-Replacement Strategy](Image)

Table I: SEC-DAED-TAED-Tetra AED hamming code (12, 8)

<table>
<thead>
<tr>
<th>Bit Placement</th>
<th>Double Adjacent Error Detection</th>
<th>Triple Adjacent Error Detection</th>
<th>Tetra Adjacent Error Detection</th>
</tr>
</thead>
<tbody>
<tr>
<td>12 3 4 5 6 7 8 9 10 11</td>
<td>12 2/11 18%</td>
<td>3/10 30%</td>
<td>0/9 0%</td>
</tr>
<tr>
<td>12 3 4 5 6 7 8 9 10 11</td>
<td>3/10 30%</td>
<td>6/9 66%</td>
<td></td>
</tr>
</tbody>
</table>

Proposed Extended SEC-DAED-TAED-Tetra AED hamming code has been detected 36.36% of Double Adjacent Error Detection (DAED), 30% of Triple Adjacent Error Detection (TAED) and 66% of Tetra Adjacent Error Detection (Tetra AED) than traditional hamming model. Further proposed extended hamming SEC-DAED-TAED-Tetra AED is incorporated into AES Encryption and Decryption algorithm. Proposed block diagram of AES Encryption and Decryption structure by using extended hamming SEC-DAED- TAED-Tetra AED has been illustrated in fig 3. Table II shows combinations of double, triple and tetra adjacent errors of proposed model.

![Figure 3: Block diagram of AES Encryption and Decryption structure by using Extended SEC-DAED- TAED-Tetra AED HAMMING Code](Image)

Table II: Possible Combination of Detecting Double and Triple Adjacent Error Combination in Both Traditional and Proposed System

<table>
<thead>
<tr>
<th>Traditional Hamming Code Number System</th>
<th>Proposed Hamming Code Number System</th>
<th>Extended SEC-DAED-TAED Code Number System</th>
</tr>
</thead>
<tbody>
<tr>
<td>Double Adjacent Error</td>
<td>Triple Adjacent Error</td>
<td>Tetra Adjacent Error</td>
</tr>
<tr>
<td>(4, 5)</td>
<td>(3, 4, 5)</td>
<td>(6, 8)</td>
</tr>
<tr>
<td>(7, 8)</td>
<td>(1, 2, 3)</td>
<td>(7, 10)</td>
</tr>
<tr>
<td>(8, 9, 10)</td>
<td>(3, 4, 8)</td>
<td>(3, 12)</td>
</tr>
</tbody>
</table>

Results and Discussions

ModelSim 6.3C is used to simulate the proposed hamming codes and AES encryption and decryption model. Figure 4 shows the simulation result of proper data transmission in AES encryption and Decryption that means hamming code indicates the status as “No Error”.

![Figure 4: Simulation result of proper data transmission in AES encryption and Decryption](Image)
Figure 4: Simulation result of proper data transmission in AES encryption and decryption

From figure 4, it is clear that hamming codes detect “No Error” in data transmission. Figure 5 shows the single error correction based AES encryption and decryption. Status of figure 5 shows “SEC”. Figure 6, 7 and 8 shows similar double, triple and tetra adjacent error detections based AES encryption and decryption model.

Figure 5: Simulation result of Single Error Correction based AES encryption and decryption

Figure 7: Simulation result of Triple Adjacent Error Detection based AES encryption and decryption

Figure 6: Simulation result of Double Adjacent Error Detection based AES encryption and decryption

Figure 8: Simulation result of Tetra Adjacent Error Detection based AES encryption and decryption

Further, proposed SEC-DAED-TAED-TETRA AED hamming codes are incorporated into AES encryption and decryption algorithm. The simulation result of AES encryption is shown in figure 9, in which 128 bits input is applied into AES encryption block. For 8-bit input data, 4 parity check bits are used to detect and correct an error. Hence, 192-bit output is obtained in AES encryption block for correcting or detecting the errors while transmitting. In decryption side, again 128 bit is decoded by using proposed SEC-DAED-TAED-TETRA AED hamming decoder. The simulation result of SEC-DAED-TAED-TETRA AED hamming code based AES decryption is shown in figure 10.

Figure 9: Hamming SEC-DAED-TAED-TETRA AED model based AES Encryption
Conclusion
In this paper, Extended Hamming Single Error Correction-Double Adjacent Error Detection-Triple Adjacent Error Detection-Tetra Adjacent Error Detection (SEC-DAED-DAED-TAED) based AES Encryption and Decryption has been designed through Very Large Scale Integration (VLSI) system design environment. Verilog Hardware Description Language (Verilog HDL) codes have been used in this paper to design and simulate the proposed hamming codes and AES algorithms. Proposed model provides both security and fault detection. Silent Data Corruption (SDC) is one of the most disadvantages of traditional hamming codes. This must be completely avoided in the proposed Extended hamming SEC-DAED-TAED-Tetra AED Code. Proposed Hamming SEC-DAED-TAED-Tetra AED codes help to improve 36.36% double adjacent error detecting probability, 30% triple adjacent error detecting probability and 66% tetra adjacent error detecting probability. Further, proposed hamming codes have been incorporated into AES Encryption and Decryption for detecting and correcting the error while encrypting and decrypting the 128-bit data. Hence, the proposed system named as Extended Hamming SEC-DAED-TAED-Tetra AED code based AES encryption and Decryption. In future, the proposed model will be well suited in mobile and internet banking for exhibiting the secure transmission.

References