# Robust code based Fault Tolerant Architecture using OFB mode for Onboard EO satellites

**G. Ramadevi, R. Sujatha**

***Abstract*— *The demand to protect the sensitive and valuable data transmitted from satellites to ground has increased and hence the need to use security algorithm on board in Earth Observation satellites also increased. The security algorithms like Advanced Encryption Standard by NIST (National Institute of Standards and Technology), is popular in the aerospace industry including satellites. The analysis of the effects of single even upsets (SEUs) on imaging data during on-board encryption is detailed. To avoid data corruption due to SEUs, fault-tolerant model of OFB mode encryption based on robust error detection and corrections codes is proposed. The satellite imaging data is encrypted using OFB mode encryption is done using Matlab. Then its encrypted output image is converted into gray codes is also done using Matlab. The gray codes with injected faults is given as an input to the proposed Robust error detection and correction code model which is designed using VHDL, from which single bit upset and multiple bit upsets are detected and corrected. The implementation of proposed model is done using Field programmable gate array (FPGA). Hence power and throughput of fault tolerant model are increased.***

***Index Terms*— *OFB mode encryption, Error detection and correction codes, Robust codes, SEUs.***

## I. INTRODUCTION

The Advanced Encryption Standard (AES), is a security algorithm which is an extension of Data Encryption Standard (DES) based on three different set of features: Mathematical structure is more complex, control path uses long keys, data path operates on large blocks of data. The software results of Output Feedback (OFB) mode encryption have been used in various fields with the aim of reducing number of clock cycles used to encrypt a data block [15].Hardware implementation using Field Programmable Gate Arrays (FPGA) is used for increasing the throughput while to reduce the number of gates and also to obtain reconfigurable elements to use with different sizes of AES for keys and data blocks. The two key issues in designing a cryptographic architecture using VLSI architecture are as follows: (i) Fault detection and (ii) Fault correction [15].The fault detection is a property for prevention of malicious attacks and targeted in getting sensitive information, For eg., Secret key from device.The fault tolerant model of OFB mode encryption is used for preventing the injection of faults.

The fault tolerant model of OFB mode encryption using non-linear robust codes(i.e.) Vasil'ev codes are used for correction of single event upsets(SEUs) and multi-bit upsets(MBUs).These non-linear codes have fewer undetectable upsets and fewer multi-bit upsets which leads to miscorrected data[6].

We present that linear Hamming codes can be replaced by non-linear Vasil'ev codes which results in improved reliability even though multi-bit upsets or error repeated in the data.

The rest of the paper is organized as follows. In Section I, OFB mode encryption for images is explained. In Section II, Overview of the proposed system is presented. In Section III, effects of SEUs are presented. In Section IV,Causes of SEUs is discussed.In Section V, Overview of Proposed system is presented.In Section VI,construction and working methods of Vasil'ev codes is described. In Section VII, we give the comparison between Hamming codes and Vasil'ev codes to understand the advantages of proposed approach. In Section VIII, OFB mode decryption for image is described. In Section IX,we conclude the paper.

## II. OUTPUT FEEDBACK (OFB) MODE ENCRYPTION FOR IMAGES

In the Output Feedback (OFB) mode encryption the output of the encryption is fed back into the input to generate a key stream, which is then XOR-ed with the plain data to generate the cipher data as in FIG.1. The key stream required for encryption and decryption process is independent of the plain and cipher data and hence the feedback propagates the faults from one block to other blocks until the end of the encryption process [9]. Each output feedback block cipher operation depends on all previous ones, and so it cannot be performed in parallel manner. However, because the plaintext or cipher text is only used for the final XOR, the block cipher operations may be performed in advance, allowing the final step to be performed in parallel once the plaintext or ciphertext is available. It is possible to obtain an OFB mode key stream by using CBC mode with a constant string of zeroes as input. This can be useful, because it allows the usage of fast hardware implementations of CBC mode for OFB mode encryption [9].

Using OFB mode encryption with a partial block as feedback like CFB mode encyption reduces the average cycle length by a factor of $2^{32}$ or more. A mathematical model proposed by Davies and Parkin and substantiated by experimental results showed that only with full feedback an average cycle length near to the obtainable maximum can be achieved. The OFB mode encryption operation can be represented by the following mathematical equation as follows:

$$Cj = Pj \oplus E(K,[C\ j\text{-}1 \oplus Pj\text{-}1]) \qquad (1)$$

In the above equation, Cj represents the ciphertext, Pj be the plaintext,E be the encrypted text function,K be the key function,Cj-1 be the previous ciphertext and Pj-1 be the previous plaintext.

The block diagram for OFB mode encryption is as follows:

**Manuscript received on May, 2013.**

**G.Ramadevi**, PG Student, Applied Electronics,Velammal Engineering College,Chennai,India

**R.Sujatha**, Assistant Professor-III, Electronics and Communication Engineering , Velammal Engineering College,Chennai,India

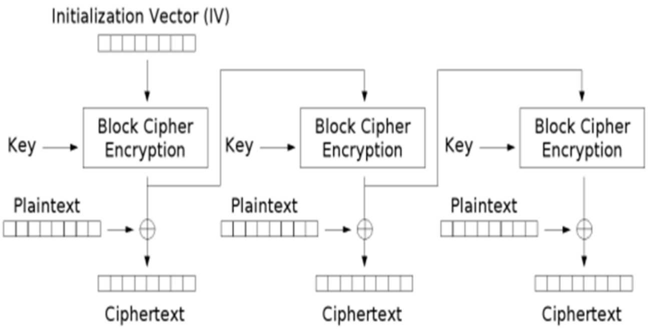

FIG.1 OUTPUT FEEDBACK MODE ENCRYPTION

Now the OFB mode encryption is very useful for onboard earth observation satellites where transmission channel are very noisy. So OFB mode encryption has many benefits and advantages when compared to other modes of AES like Cipher block chaining mode(CBC) and also Cipher feedback mode(CFC) because any bit upsets occurs in cipher data are not propagated to affect the decrypted subsequent block[9].

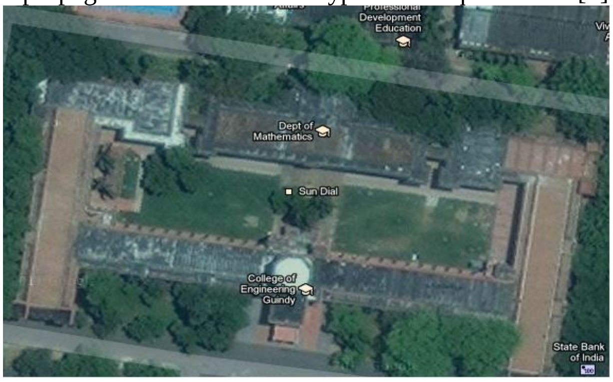
Professional Development Education
Dept of Mathematics
Sun Dial
College of Engineering Guindy
State Bank of India

FIG.2 SATELLITE INPUT IMAGE

The FIG.2 is a satellite image of Anna university which is taken from the goggle search engine is given as input to OFB mode encryption. The main advantage of OFB mode is that it has high-speed for processing of input data. It also consumes less time for processing of plain data. The plain/input data are XOR-ed with precomputed keystream to form encrypted data when they are transmitted from satellite to ground[9].

Then the input satellite after given as an input to the OFB mode will produce encrypted output image which is shown in following FIG. 3.

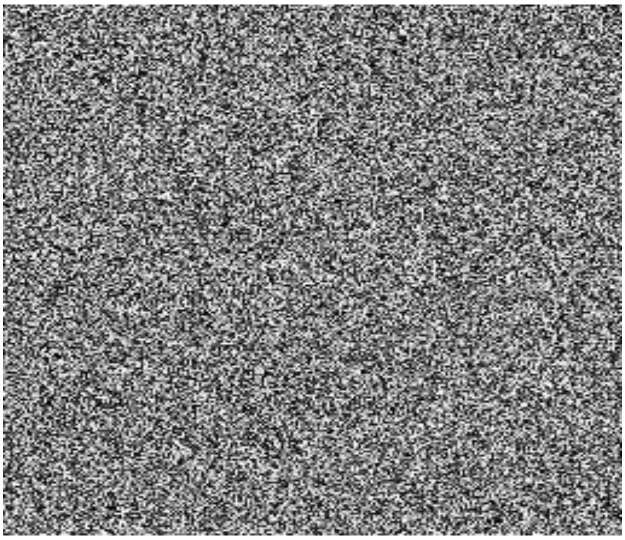

FIG.3 ENCRYPTED OUTPUT IMAGE

## III. SINGLE EVENT UPSETS (SEUS)

A **single event upset** (**SEU**) is a change of state caused by ions or electro-magnetic radiation striking a sensitive node in a micro-electronic device, such as in microprocessor, semiconductor memory,of power transistors,etc.The state change is a result of the free charge created by ionization in or close to an important node of a logic element(e.g. memory "bit"). The error in device output or operation caused as a result of the strike is called an SEU or a soft error. The SEU itself is not considered permanently damaging to the transistor's or circuits' functionality unlike the case of single event latchup (SEL), single event gate rupture (SEGR), or single event burnout (SEB). These are all examples of a general class of radiation effects in electronic devices called single event effects.

## IV. CAUSES OF SINGLE EVENT UPSETS (SEUS)

Terrestrial SEUs arise due to cosmic particles colliding with atoms in the atmosphere, creating cascades or showers of neutrons and protons, which in turn may interact with electronics. At deep sub-micrometre geometries, this affects semiconductor devices in the atmosphere.In space, high energy ionizing particles exist as part of the natural background, referred to as galactic cosmic rays (GCR). Solar particle events and high energy protons trapped in the Earth's magnetosphere (Van Allen radiation belts) exacerbate the problem. The high energies associated with the phenomenon in the space particle environment generally render increased spacecraft shielding useless in terms of eliminating SEU and catastrophic single event phenomena (e.g. destructive latch-up). Secondary atmospheric neutrons generated by cosmic rays can also be of energies capable of producing SEUs in electronics on aircraft flights at high altitude.Table 1 shows the comparison between CBC and OFB modes of AES:

TABLE 1 COMPARISON BETWEEN CBC AND OFB MODES

| **SOURCE OF ERROR** | CBC | OFB |
|---|---|---|
| During encryption on- board | One block | All data after the point of fault occurrence |
| During transmission | Two blocks | No fault propagation |

## V. OVERVIEW OF PROPOSED SYSTEM

The Overview of the proposed system is shown in the following FIG.4. The block diagram of the proposed system consists of OFB mode encryption, gray codes, memory, then decoder consists of error detection and correction codes and decryption.

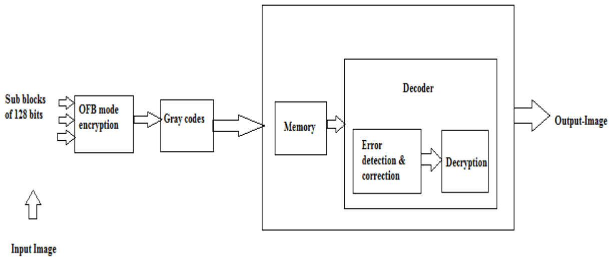

FIG.4 OVERVIEW OF THE PROPOSED SYSTEM

The input image is divided into sub-blocks of 128 bits. Then it is given as an input to OFB mode encryption block, designed using MATLAB. The encrypted image after encryption is given to graycode conversion block which is designed using MATLAB, due to this gray code conversion speed of cryptographic processor is increased and it also increases the throughput of fault tolerant based on robust codes. The gray code values from gray code block is given to memory. Then it given as input to the error detection and correction block, designed using VHDL.If any errors occurs in the data, then it will be rectified with the help of Vasil'ev code called robust code.The output of which is decrypted using OFB mode decryption which is designed using VHDL.

## VI. ROBUST ERROR DETECTION AND CORRECTION CODES

The proposed fault-tolerant model is based on the protection based on nonlinear systematic robust codes which can provide for uniform protection against all errors without making any assumptions about the error and capabilities of an attacker. The Robust constructions are based on perfect or almost perfect nonlinear functions which are an integral part of many cryptographic algorithms[10]. The Robust constructions can be applied to existing architectures based on linear error-detecting codes to redistribute their error detecting power and reduce the number of undetectable errors. The paper presented here is an example application of the robust codes construction to an implementation of the hardware for OFB mode Encryption Standard in Onboard Earth Observation Satellites, secure against fault attacks. Architectures based on these robust constructions have fewer undetectable errors than linear codes with the same n, k. These nonlinear codes are capable of providing uniform error detecting coverage independently of the error distributions. This proposed error-detecting codes have the advantage of an increased probability of detecting jamming attacks and permanent failures which result in repeating errors. For linear codes, if a hardware failure (say, from tampering) produces a fault within a circuit which results in a repeated error which is a codeword the fault will always be undetected. For the Robust code, which has data dependent detection, any repeating error, will eventually be detected.

The Vasil'ev codes are used to detect and correct errors in encrypted data based on Syndrome values.The syndrome values are given by the following equations:

$$S1 = C1! + C2! \qquad (2)$$

$$S2 = C1! + C2! + C3! \qquad (3)$$

$$S3 = C1! + C2! + C3! + C4! \qquad (4)$$

### VI.(A) VASIL'EV CODE ALGORITHM FOR ERROR DETECTION AND CORRECTION :

Steps to detect and correct any kind of errors using Vasil'ev codes are as follows;

1. If all S is zero, then no error occurs in data.

2. S3= 0 & one of S1,S2 is not zero,errors with even multiplities are detected.
3. S3=1 & S1=0,a single bit error are detected.
4. S3=1,S1 is not zero,errors of odd multiplicities are detected and corrected.

## VII. COMPARISON BETWEEN HAMMING AND ROBUST CODES

The following Table 2 show the comparison between hamming and vasil'ev codes based on the error detection and correction capability and also on the security they provide to the input from satellite to ground

TABLE 2 COMPARISONS BETWEEN HAMMING CODES AND VASIL'EV CODES

| Hamming codes | Vasil'ev codes |
|---|---|
| Hamming codes also called as linear codes | Robust codes also called as nonlinear codes |
| Detect errors with small multiplicities(or errors of particular type) | Provide equal protection against all errors(small or large multiplicities) |
| Provide little prote ction | Provide protection for both private & public key cryptosystems. |

## VIII. OFB MODE DECRYPTION

The OFB mode decryption is done to check the whether the data is correctly received without any errors. The OFB mode decryption is given by the following equation:

$$Pj = Cj \oplus E(K,[Cj-1 \oplus Pj-1]) \qquad (5)$$

In the above equation, Cj represents the ciphertext, Pj be the plaintext, E be the encrypted text function,K be the key function,Cj-1 be the previous ciphertext and Pj-1 be the previous plaintext.

The data from error detection and correction codes are given as input to the OFB mode decryption. The decrypted image is nothing but the input image what we given as an input data to the fault tolerant before encryption. Thus the satellite image is obtained as output image after decryption. In OFB mode decrypted ouput,there is no propagation of faults from satellite to ground,so OFB mode is more suitable for Onboard earth observation (EO)satellites. Then OFB mode decrypted image is shown in the following FIG. 6.

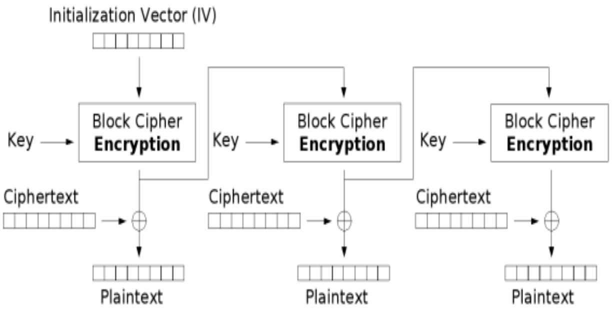

FIG. 5 OFB MODE DECRYPTION

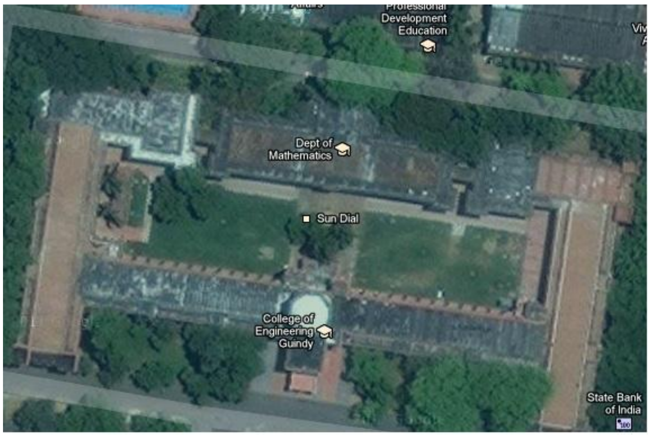
Professional Development Education
Dept of Mathematics
Sun Dial
College of Engineering Guindy
State Bank of India

FIG. 6 OUTPUT IMAGE

## IX. CONCLUSION

The OFB mode encryption is used in the fault tolerant model of proposed system is one of the standard modes of encryption standard issued by NIST(National Institute of Standards and Technology).The impact of the propagation of SEU faults during on-board encryption is presented. OFB mode encryption model provides no error transmission from satellite to ground. Thus it is more suitable for Onboard EO satellites.The model can be extended for detection and correction of single as well as multiple bit upsets.The proposed fault detection and correction of OFB mode encryption model targets the satellite application domain, however it can also be used in other applications aimed at hostile environments such as nuclear reactors, interplanetary exploration, unmanned aerial vehicles, etc. Terrestrial applications, which require a high level of reliability and security, such as bank servers, telecommunication servers, etc. can benefit from the use of AES fault-tolerant techniques too.

## REFERENCES

[1] Praveen.H.L , H.S Jayaramu, M.Z.Kurian,"Satellite Image Encryption Using AES" International Journal of Computer Science and Electrical Engineering (IJCSEE) ISSN No. 2315-4209, Vol-1, Iss-2, 2012

[2] Praveen.H.L, H.S Jayaramu & M.Z.Kurian,"Single Event Upset Correction for Satellite Images by using AES" International Conference on Electronics and Communication Engineering, 20th May 2012, Bangalore,ISBN: 978-93-81693-29-2

[3] Z.Wang and M.G.Karpovsky(June 2012)"Reliable and Secure Memories Based on Algebraic Manipulation Correction Codes", Proc Int Symp. on On-line Testing.

[4] Z.Wang and M.G.Karpovsky,(2012)"New Error Detecting Codes for design of Hardware Resistant to Strong Fault Injection Attacks", Proc. Int. Conference on Security and management, SAM.

[5] T.Mangaiyarkarasi and B.Nandhini **(**March 2012)"Fault and tolerant method using AES for images",International Journal of Communications and Engineering,Vol.05,No.5,Issue:01,

[6] K.D.Akdemir, Z. Wang, M. G. Karpovsky, and B. Sunar**,** (2011) "Design of Cryptographic Devices Resilient to Fault Injection Attacks Using Nonlinear Robust Codes", Fault Analysis in Cryptography, M. Joye Editor.

[7] Z. Wang, M. G. Karpovsky, K. Kulikowski, "Design of Memories with Concurrent Error Detection and Correction by Non-Linear SEC-DED Codes", Journal of Electronic Testing, vol. 26, Oct 2010.

[8] Z. Wang, M. G. Karpovsky, K. Kulikowski,(July 2009),"Replacing Linear Hamming Codes by Robust Nonlinear Codes Results in Reliability Improvement for Memories", Proc. Int. Symp. Dependable Computing.

[9] Roohi Banu and Tanya Vladimirova (January 2009) "Fault-Tolerant Encryption for Space Applications"**,**IEEE transactions on Aerospace and Electronic Systems Vol. 45, No.1,(266-279).

**[10]** Konrad.J, Kulikowski, Mark.G.Karpovsky, and Alexander Taubin(2007) "Robust codes and robust, fault tolerant architectures of the advanced encryption standard",ELSEVIER, Journal of System Architecture, Vol.53,(139-149).

[11] M.G.Karpovsky,K.Kulikowski,Z,Wang,"Robust Error Detection in Communication and Computation Channels",(2007) Keynote paper, Int. Workshop on Spectral Techniques.

[12] Vladimirova.T, and Banu.R(Sept. 2005),"On-board security services in small satellites".In Proceedings of the 8th Military and Aerospace Applications of Programmable Logic Devices and Technologies International Conference (MAPLD'2005), F-184, NASA, Washington, D.C.

[13] Mark Karpovsky, Konrad J. Kulikowski, Alexander Taubin**(**2004**)"**Differential Fault Analysis Attack resistant Architectures for the Advanced Encryption Standard" ,In: Ser. Proc. IFIP world computing congress,Cardis,pp (177-193)

[14] M.G.Karpovsky and A. Taubin,(2004)"A New Class of Nonlinear Systematic Error Detecting Codes", IEEE Trans Info Theory, Vol 50, No.8, pp.1818-1820

[15] Karpovsky, M.G., K. Kulikowski, and A. Taubin,(July, 2004) "Robust Protection Against Fault-Injection Attacks on Smart Cards Implementing the Advanced Encryption Standard", Proc. Int. Conference on Dependable Systems and Networks (DNS 2004).

[16] Bertoni.G, Breveglieri.L, Koren.I, Maistri.P, and Piuri.V. (Apr. 2003) "Error analysisand detection procedures for a hardware implementation of the AES",IEEE Transactions on Computers, Vol.52, 4, 493-505.

[17] Behrouz A.Forouzon and Debdeep Mukhopadhyay,2nd Edition, Crytography and Network Security, Tata Mcgraw Hill Education Pvt. Limited.

[18] William Stallings,5th Edition,Cryptography and Network Security, Principles and Practice, Pearson.

[19] Charlie Kaufman,Radia Perlman,and Mike Speciner,2nd Edition,Network Security, Private Communication in a Public World, Pearson Education.

[20] Input image from Google Search engine