Joint encryption and error correction schemes: A survey

R.V. Chothe[1], S.P. Ugale[2] , D.M. Chandwadkar[3], S.V. Shelke[4]
[1,2,3,4] Department of Electronics and Telecommunication Engineering, K.K.Wagh Institute of Engineering Education and Research, Savitribai Phule Pune University, Pune, India

Article Info

Article history:
Received Aug 2, 2024
Revised Nov 7, 2024
Accepted Nov 21, 2024

Keywords:
Error-free transmission
Crypto-coding
Encryption algorithms
Literature survey
Cryptography

ABSTRACT

In this recent era, the sharing of critical information is essential. Along with information security, error-free data transmission is equally important. Crypto-coding is the method combining encryption algorithms and error correcting codes to enhance performance in terms of security, time, resources, or complexity. Despite the significant research, a comprehensive systematic literature survey that explores the status of research is not available. The proposed study fills this gap by exploring the available research in detail and highlighting past contributions, allowing readers and upcoming researchers to have a detailed understanding of various software and hardware implementations of crypto-coding algorithms and their results. This paper presents a comparison of encryption methods based on various parameters. The crypto-coding research work in satellite communication is also added. The survey includes implementation methods, results, applications, and comparisons of previous work results. This systematic literature survey also covers open issues and future trends of solutions in this context. The paper will offer directions for potential research in the area of crypto-coding and will expand the research frame for upcoming scholarly research.

Corresponding Author:
R.V. Chothe
Department of Electronics and Telecommunication Engineering,
K.K.Wagh Institute of Engineering Education and Research,
Savitribai Phule Pune University, Pune, India.
ORCID: 0009-0001-2235-1309.
Email: rvchothe@kkwagh.edu.in

1. INTRODUCTION

For many different applications, including banking, military uses, satellite communications, medical industry, and many more, data security is becoming more and more important. It is crucial yet challenging to prevent unauthorised parties from discovering or altering any communication taking place through various means, including the internet. Cryptography is the most significant method for information security. It is a method for securing network-based data delivery. It enables us to transfer or store sensitive data securely over open networks without worrying about hackers reading it. Symmetric and asymmetric cryptographic systems have already been developed and are currently used widely [1].

In the past, various encryption methods like DES were employed as the main security measures for data concealment. However, there are some weaknesses in each of these techniques, which is why there are so many data breach cases. Through either a passive or active attack, information can be altered or hacked. Symmetric encryption methods include Data Encryption Standard (DES), Triple DES, and Advanced Encryption Standard (AES). The data is encrypted and decrypted at both ends using a key that is shared by the transmitter and receiver [2]. Rivest-Shamir-Adleman algorithm (RSA), Elliptic Curve Cryptography (ECC), and Digital Signature Algorithm (DSA) are asymmetric cryptography methods, employing different keys for encryption and decryption.

In the modern era, symmetric cryptography is far more suitable for protecting massive amounts of data. The DES algorithm has been replaced by the AES algorithm developed by the National Institute of Standards and Technology (NIST) [3]. The use of AES was proposed by the Consultative Committee for Space Data Systems (CCSDS) and the NIST [4] [5]. There are numerous operational modes for the AES algorithm [6].

When the data is transmitted through wireless channels, there are chances of error. The signal transmission power can be increased to improve the reliability of signal transmission. Error correction coding is the method providing reliability without rise of signal power. In the conventional implementations, encryption and coding are independent. In traditional GSM, encryption is done after encoding [7].This complex method increases the delay. These methods are not suitable to cater high speed and high security requirements of emerging technologies like 5G and 6G. The computational complexity can be reduced to reduce latency [8]. But, if the combination of encryption and encoding is not properly achieved, the communication can be hampered [9]. Thus, it is essential to research on proper merge of encoding with cryptographic algorithms and to design new schemes providing high security along with error free transmission.

As compared to the other algorithms, AES is more secure [10]. So, AES is a perfect candidate for recent applications [11] [12]. AES has some limitations in case of predictable patterns in subkey generation and the sharing of secret key [13]. So, the researchers have modified basic AES algorithm for better security and performance.

Thus, cryptography and coding theory play a pivotal role in advanced applications. However, research combining both these concepts is a crucial topic of interest that forms the base of this literature review. Past reviews in the field of cryptography, such as [14] and [15], are not sufficient as per the range of time covered and scope. They are only based on encryption methods. They do not cover the whole research on crypto coding combined work and the performances. Despite the research and studies in the fields of cryptography and encoding, a comprehensive systematic literature survey (SLS) on crypto-coding is not available. The presented paper filled this gap by examining the research in a broader way. Thus, a survey summarizing the research to direct readers, researchers, academicians, and industry experts for implementation or further research is presented.

The research outcomes of the presented survey are:

1. The detail comparison of available encryption methods based on implementation is presented. AES outperforms all other block encryption schemes.
2. Early phase of research in cryptography is surveyed to create the background.
3. AES implementations on various platforms along with implementation details and their results are discussed.
4. Crypto-coding using AES and various error correction schemes is surveyed. The performance improvement as compared with previous research and gaps in present papers are also added in the table form.
5. Implementation of AES and crypto coding methods for satellite applications are surveyed.
6. Research efforts for reduction of attacks are summarized.
7. Directions for future research is provided for upcoming researchers.

2. PERFORMANCE COMPARISON OF ENCRYPTION METHODS

Cryptography techniques are divided into two categories: symmetric and asymmetric, depending on how many keys are needed for protect and retrieve data. The security depends on the size of the key used. The sharing of a symmetric key between the sender and recipient adds the limitation to symmetric algorithms. The symmetric key cryptography algorithms that are representative are RC2, DES, 3DES, RC5, Blowfish, and AES. The symmetric key algorithms are further categorized into stream ciphers (RC4, Salsa20), which operate bitwise on the data, and block ciphers (AES, Blowfish), which operate on blocks of a predetermined length. Figure 1 shows minimum and maximum key sizes for different algorithms. Asymmetric algorithms use two different keys. Because asymmetric algorithms require high processing power than symmetric methods, they are nearly a thousand times slower [16]. Asymmetric algorithms avoid the risk of key sharing. The researchers have implemented and compared both symmetric and asymmetric methods using different types, contents and sizes of input files. The algorithms are compared based on parameters such as memory requirement, processing time, and throughput. The algorithms are implemented on different platforms and simulation results are presented.

The cipher block chaining (CBC) mode of the AES/DES/Blowfish algorithms was used with keys of 64 bits, and 128 bits. It was simulated on a laptop running Windows 64-bit, an i3 processor running at 1.90 GHz, and 4 GB of RAM [17]. Random text and image files of 1, 2, 5, and 20 MB were created to check the performance. The system was implemented using Java 1.7.0. Ten rounds were performed on each data block. Figure 2 plots encryption time required by AES, DES, RSA and Blowfish algorithms. Throughput (KB/mSec) is the size of plain text divided by the processing time. The results conclude that the throughput of AES is better than the other three algorithms and RSA is most time consuming. [17], [18].

Reviewing the RSA, AES, and DES algorithms revealed that the performance and speed of asymmetric methods are significantly lower than those of symmetric encryption techniques like AES. Additionally, asymmetric algorithms like RSA and Diffie-Hellman are typically utilised for symmetric encryption, like AES secret key exchange, as well as digital signatures and non-repudiations. Symmetric methods are useful to secure bulk data like data base encryption, and asymmetric methods will serve the secure key transfer of the symmetric algorithms, the integrity check and non-repudiation. RSA implementations consume high computational resources [15].

To evaluate which secret key algorithm provides the best performance, a study on various algorithms was conducted [19]. The study focused on four widely used methods, Blowfish, AES, DES, and 3DES. Two different platforms, P-II 266 MHz and P-4 2.4 GHz, were used for testing. The findings indicate that AES provides better performance than 3DES and DES.

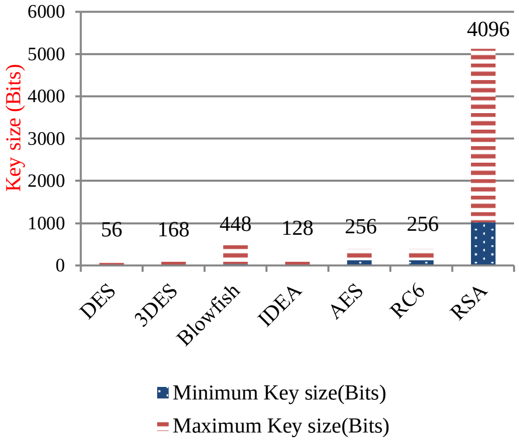

Figure 1. Minimum and maximum key sizes for different algorithms [20]

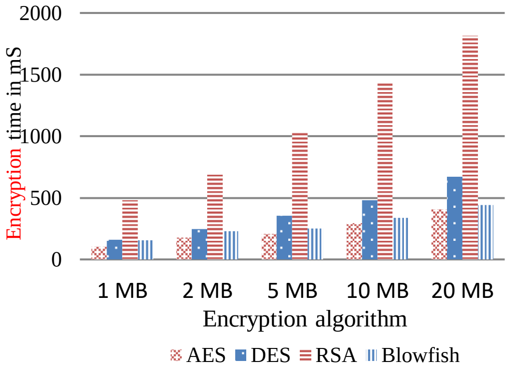

Figure 2. Encryption time comparison of algorithms with 10 rounds, implemented on system with Windows 64-bit, i3 processor running at 1.90 GHz [17]

The performance of six techniques AES, DES, 3DES, RC2, Blowfish, and RC6 was evaluated in [21]. Different variables were applied to each method to compare them, such as data types and sizes, key sizes, power consumption, and processing speeds. The analysis revealed that the AES outperformed Blowfish with a speed difference of 200–300 milliseconds. Blowfish can perform better when the packed size changes, followed by RC6. RC2 was maximum time consuming. Compared to RC2, DES, and 3DES, AES offered a superior performance. However, it is evident from the results that as key size grows, so do battery and time requirements [21]. In [18], three encryption methods, including AES, DES, and RSA were analyzed. The processing time and memory consumption for text files were checked. The findings demonstrated that RSA requires more processing time and higher amount of memory than the AES and DES.

Thus, the research work including the implementation of various cryptographic algorithms and their results is reviewed. The best cryptographic technique for encrypting large amounts of data with the least amount of hardware resource usage is AES. Additionally, several modifications to the fundamental algorithm can be made to enhance performance.

3. HISTORY OF CRYPTOGRAPHY/EARLY PHASE OF RESEARCH IN CRYPTOGRAPHY

The earlier research concentrated on the joint encryption and error correction scheme, which embeds security into the error correction code to increase overall system security by preventing an attacker from correcting channel errors without knowing the secret keys and preventing them from decrypting the transmitted data.

Goppa code was utilised by McEliece [22] in 1978 to create the quick-encrypting M public-key cryptosystem. However, because the key size is too high, the system cannot defend against cipher text-only attacks. A Joint encryption and error correction system [23] based on (N, K) linear block coding was first proposed by Rao. The algorithm was modified by adding a random error vector. Niederreiter developed N public key crypto system in 1986 [24].

The analysis of chosen plaintext attacks on the Rao- Nam (RN) method revealed that it is unsafe. This attack works by solving a series of linear equations to estimate the rows of the encryption matrix. In [25], Struik put up a modified strategy in which an invertible nonlinear function, f, would take the place of the scrambling matrix. However, this plan is unable to combine security with reliability. To protect the system from intrusions, Rao and Nam developed a syndrome-error table in 1989 [26]. Another block chaining-based strategy has been presented in [27] as secret error correcting code (SECC). But the random error word added to original word is of low Hamming weight, so the security can be hampered.

Data Encryption Standard (DES) was used in the past. NIST issued an invitation for suggestions in January 1997 for the creation of innovative, sophisticated, and secure algorithms for the AES. The Rijndael algorithm was selected as the AES algorithm by NIST in October 2000 after two iterations of examination on the 15 candidate algorithms. Dedicated hardware can be used to deliver much higher speeds, greater physical security, and reduced power consumption as compared to software. The researchers created a nonlinear system, Error Correction Based Cipher (ECBC), a secret error-correcting code [28]. The nonlinear function used in this technique is susceptible to differential attacks since it is similar to the substitution box (S-box) of the AES [29].

4. SURVEY OF AES IMPLEMENTATIONS AND MODIFICATIONS

The researchers have implemented the AES algorithm using various software and hardware platforms and presented their results. The software implementations include MATLAB or Modelsim. The encryption systems are also developed using SPARTAN FPGA boards with XILINX-ISE software. The available research work and its implementation details are discussed here.

The fundamental AES algorithm was changed by few researchers. In order to achieve a small hardware architecture, the S-box was optimized. The compact implementation of a merged S-box in [30] is 20% more compact than the previous most compact version of [31]. The multi-level GF (2^8) representation of arithmetic is used in this approach. Some of the XORs and NANDs have been swapped out for NORs. But in this work, the problems of timing, latency, and delay are not examined. The summary of the research work discussed is added in Table 1. It also highlights the results of the implementations.

Table 1. Review of AES implementations on various platforms and their results

Ref. No.	Year	Implementation methods	Results
[39]	2012	• Xilinx's SPARTAN-3 FPGA.	• Higher throughput rate of 4.25% than basic AES pipeline structure • 56% Hardware saved.
[40]	2013	• Xilinx SPARTAN-3E (XC3S500E-FG320) • Mixing of software-hardware platforms using Micro blaze processor	• Less execution time: 2.06 sec • Less power consumption: 0.513 Watts
[41]	2016	• MATLAB HP notebook • 64bit OS, i5 processor.	• 87 ms for encryption and 88 ms for decryption. • Key setup time from 1.16 ms to 1.61 ms.
[32]	2016	• FPGA	• Less number of slices, no. of Flip Flops, LUTs used
[42]	2016	• AES designed using VHDL • FPGA network card NFB-40G2 with Virtex-7.	• Average speed 5100 Mbit/s.
[43]	2018	• MATLAB	• Reduced distortion.
[44]	2018	• Simulation using ModelSim • Xilinx FPGA board XC6SLX451	• 3854 slices of FPGA used, • 153.3 MHz frequency with 1.57 Gbps throughput • Resistance to 1st order differential power attack
[45]	2002	• Xilinx FPGA board XC2V3000	• 7617 slices of FPGA used • 0.876 Gbps throughput with 75.3 MHz frequency
[46]	2011	• Xilinx FPGA board XCVLX50 • S-Box with 65 4-input LUTs and 33 slices • Three-layered pipelining system	• 4992 slices of FPGA used • 1.35 Gbps throughput with 116 MHz frequency.
[47]	2018	• Intel Pentium 4 • Xilinx 14.7 and Model SIM. • SPARTAN 6 FPGA with XC6SLX-9TQG144 board	• Operating frequency of 291.68 mhz • Throughput up to 37.21 Gbps
[48]	2019	• ModelSim-Altera 6.4a • Xilinx ISE14.7 • Virtex-6 XC6VLX240T FPGA kit	• Clock frequency of 276.031 MHz.
[49]	2020	• AES- New Instructions(NI) • Verified using online randomness and entropy tester, and the Statistical Test Suite from NIST	• 13.5x speed over AES • 90% reduced energy consumption
[50]	2024	• AES-GCM (galois counter mode) with nonce and RSA algorithm	• 290.80, 3101.27, and 32.42 times more throughput than AES+RSA, AES, RSA

The xc2s250e component was used to implement AES on the SPARTAN3E FPGA chip. The input is in ASCII, which is just plain text. The given data is converted from ASCII to hexadecimal, and then the AES algorithm's several phases are used to turn it into cipher text. [32] Many researchers have developed the

AES algorithm using multiple lookup tables on FPGA. The two benefits are a smaller code base and more effective implementation [33].

For IoT Edge devices, Xilinx System Generator and SPARTAN-6 FPGA board were used for hardware and software co-simulation of AES-128. Results for image encryption and decryption were successful using MATLAB 2011a [34].The security of medical information was increased using improved AES in [35].The input data was initially scrambled and applied to AES. Last round of AES was modified. The encryption time was reduced and the results are proved using different volumes of data. Actual AES is designed based on Binary Galois Field. The similar structure as AES was presented in [36] using inverse property loop. The comparatively simpler structure offered high randomness. The resistance against cryptanalytic attacks was proved.

The performance of a polymorphic AES was investigated in [37]. The basic AES operations of substitution of bytes, rows shifting and mixing of columns is made key dependent. The Kerckhoff's principle is satisfied and for every different key, the basic operations will produce different output. The index values for bytes substitution, row shifting and column mixing will be derived from particular byte value of the key using mod operations. Equation 1 presents basic AES shift row operation. Equation 2 shows the polymorphic shift rows operation for index value of 3. Here, the third row is not shifted. Consecutive rows will be shifted by 1, 2 and 3 positions. The Substitution of Bytes and Mixing of Columns are also dependant on key index values. Thus, static nature of the AES is changed to dynamic. The cipher passes all NIST tests. The key avalanche and plaintext avalanche achieved were 0.495 and 0.504 respectively [37]. The researches like [38], [44], [36] and [37] worked to improve security performances of AES. Other enhancement objectives are listed in Table 2.

$$\begin{bmatrix} S_{0,0} & S_{0,1} & S_{0,2} & S_{0,3} \\ S_{1,0} & S_{1,1} & S_{1,2} & S_{1,3} \\ S_{2,0} & S_{2,1} & S_{2,2} & S_{2,3} \\ S_{3,0} & S_{3,1} & S_{3,2} & S_{3,3} \end{bmatrix} \rightarrow \begin{bmatrix} S_{0,0} & S_{0,1} & S_{0,2} & S_{0,3} \\ S_{1,1} & S_{1,2} & S_{1,3} & S_{1,0} \\ S_{2,2} & S_{2,3} & S_{2,0} & S_{2,1} \\ S_{3,3} & S_{3,0} & S_{3,1} & S_{3,2} \end{bmatrix} \tag{1}$$

$$\begin{bmatrix} S_{0,0} & S_{0,1} & S_{0,2} & S_{0,3} \\ S_{1,0} & S_{1,1} & S_{1,2} & S_{1,3} \\ S_{2,0} & S_{2,1} & S_{2,2} & S_{2,3} \\ S_{3,0} & S_{3,1} & S_{3,2} & S_{3,3} \end{bmatrix} \rightarrow \begin{bmatrix} S_{0,1} & S_{0,2} & S_{0,3} & S_{0,0} \\ S_{1,2} & S_{1,3} & S_{1,0} & S_{1,1} \\ S_{2,3} & S_{2,0} & S_{2,1} & S_{2,2} \\ S_{3,0} & S_{3,1} & S_{3,2} & S_{3,3} \end{bmatrix} = \begin{bmatrix} S'_{0,0} & S'_{0,1} & S'_{0,2} & S'_{0,3} \\ S'_{1,0} & S'_{1,1} & S'_{1,2} & S'_{1,3} \\ S'_{2,0} & S'_{2,1} & S'_{2,2} & S'_{2,3} \\ S'_{3,0} & S'_{3,1} & S'_{3,2} & S'_{3,3} \end{bmatrix} \tag{2}$$

Table 2. Research outcomes summary of AES implementations

Ref. No.	Year	Improvements related with		
		Hardware	Speed	Power consumption
[39]	2012	✓	✓	
[40]	2013	✓	✓	✓
[51]	2015			✓
[32]	2016	✓		
[42]	2016		✓	
[44]	2018	✓	✓	
[45]	2002	✓	✓	
[46]	2011	✓	✓	
[52]	2018		✓	
[47]	2018		✓	
[48]	2019		✓	
[49]	2020		✓	✓
[53]	2021		✓	
[45]	2023		✓	
[50]	2024		✓	

5. CRYPTO-CODING IMPLEMENTATIONS

Data confidentiality and reliability issues have been major concerns in advanced digital infomation systems. As the devices are becoming fast and resource-constrained, improving resistance to attacks without raising hardware complexity or computational costs is essential. One way to help meet the security and speed requirements is to provide security and reliability of transmitted data in a single system with less processing complexity.The National Scientific Foundation of the USA established a committee to study the scenario and consequences of combining cryptography and error correction. The effecectiveness of crypto-coding was highlighted as the result, but particular coding technique was not mentioned [54]. Figure 3 shows conventional communication system where channel coding/error correction coding coding follows encryption. Figure 4 represents crypto-coding system where the combined block provides both data security and reliability.

The reduction in encryption-decryption time is achieved in [53] using the structure shown in Figure 5. The input image data is divided in 128 bits and applied to basic AES. 8 iterative rounds are performed on data using initial key K_1. Output 128 bits will be fed directly to LDPC encoding mechanism. LDPC code block size calculation time is saved. Rate ½ LDPC generates 256 bit data which is added with second key of 256 bits. Here, 2 rounds of AES are reduced. So, processing time-gain is achieved. The security is verified using Entropy, Correlation and histograms. The image is recovered at SNR more than 2 dB. The performance of crypto-coding system is verified using MATLAB.

The key sharing problem of symmetric AES is handled in [13]. The actual encryption key is extracted from shared key using neural key exchange protocol, avoiding need to share original key in cloud storage. Figure 6 shows the crypto-coding block diagram. Initial 9 rounds are similar to basic AES and LDPC is incorporated in 10th round as shown in Figure 7. The results are verified using the structural similarity index (SSIM) and peak signal-to-noise ratio (PSNR) and they are better than the results of [55] and [56].

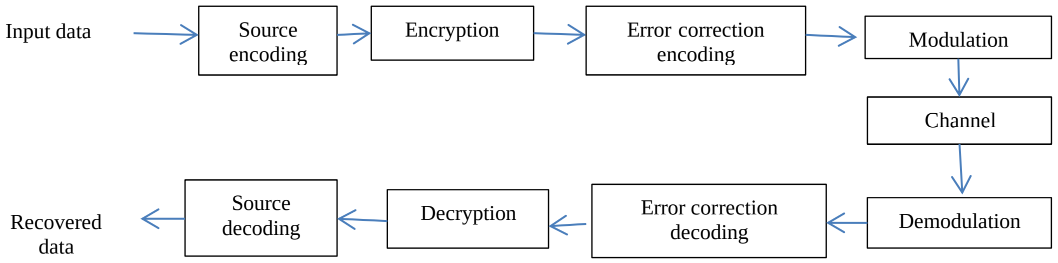

Figure 3. Structure of conventional communication system

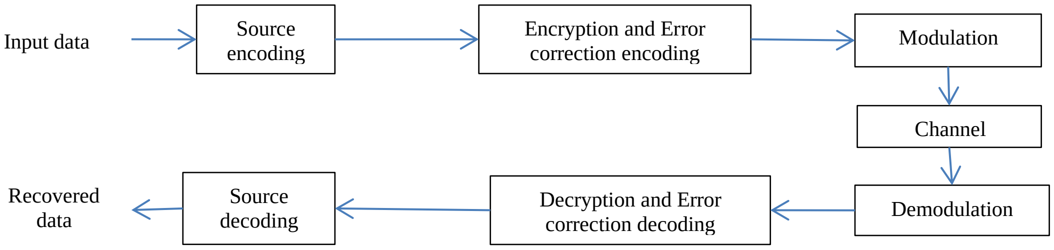

Figure 4. Modified Structure of crypto-coding based communication system

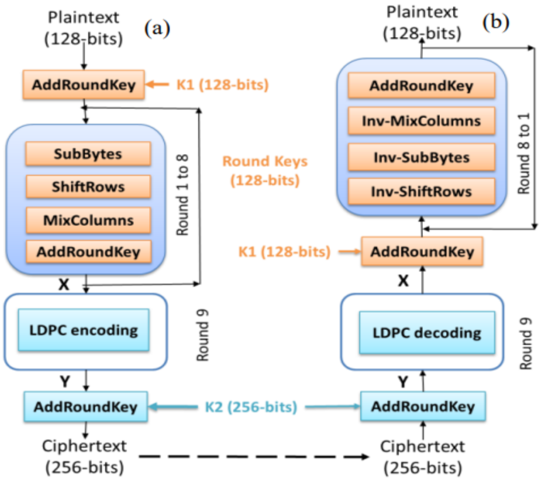

Figure 5. The joint AES –LDPC crypto system structure [53]

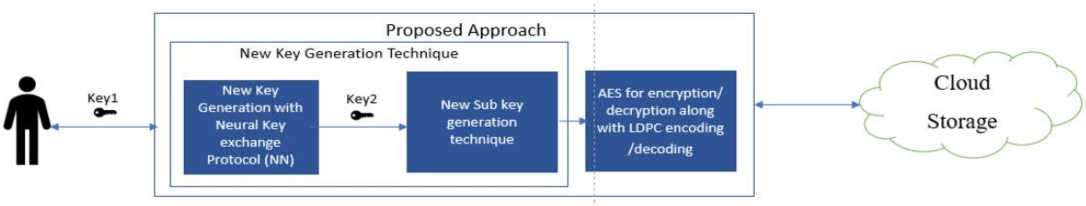
Proposed Approach
New Key Generation Technique
Key1
New Key Generation with Neural Key exchange Protocol (NN)
Key2
New Sub key generation technique
AES for encryption/ decryption along with LDPC encoding /decoding
Cloud Storage

Figure 6. Neural crypto coding for cloud storage using AES and LDPC [13]

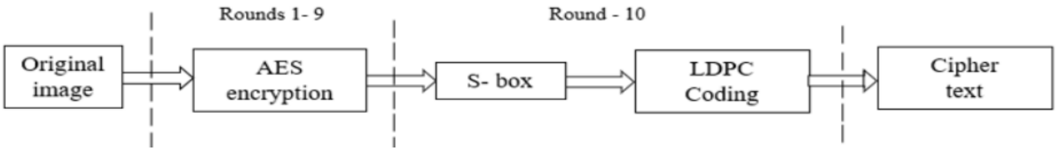

Figure 7. AES LDPC coding [13]

As shown in Figure 8, whole communication system along with crypto-coding, modulation and channel transmission was implemented in [57]. Data scrambler was added for additional security. Second 128 bit key was added during AES rounds. (648,486) rate ¾ LDPC was incorporated with AES-256 before scrambling operation. The entropy, correlation and histogram analysis prove that the algorithm is providing high security.

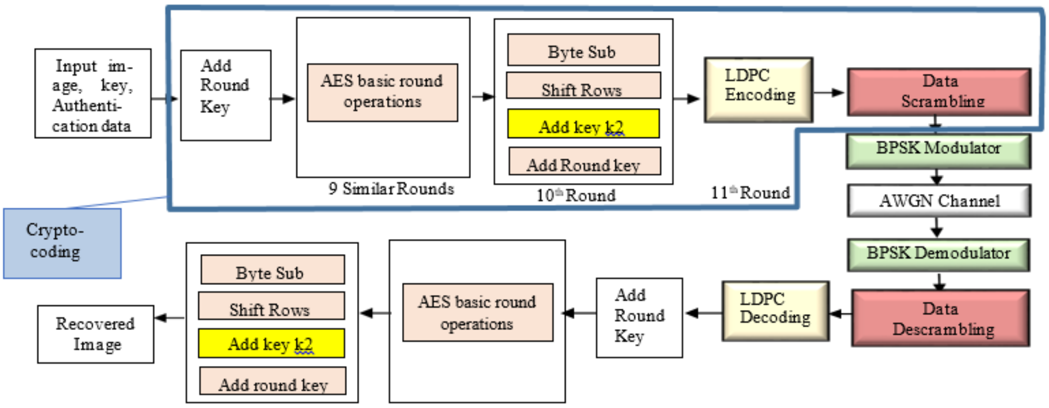

Figure 8. Crypto-coding transmission system proposed in [57]

Recent study evaluated the performance of AES together with Generative AI to protect private messages on social media platforms. [58]. Turbo codes are used in crypto-coding applications for image encryption. The BER performance is improved and security is proved using correlation graphs and histogram plots [59], [60]. Combined scheme of AES and LDPC provides advantages in terms of power reduction. Error resilience with less than 20% data rate degradation is achieved [51]. But the algorithm has higher computational complexity. Also resistance to differential power analysis is not checked.

The Communications in noisy channel is secured using hyper chaotic system and LDPC+AES cryptocoding in [61]. The system is implemented on MATLAB. NIST SP 800-22 tests were conducted. The system is immune to Differential attack. In [62], researchers have developed a framework for secure access to medical images based on an improved AES algorithm. The methodology uses Hash function for designing Dynamic S-Box generation. It is shown that the system is faster than standard S-Box generation.

A hyper chaotic system is a chaotic mathematical model in cryptography that has several positive Lyapunov exponents. It produces extremely complex and unpredictable sequences that are used to create encryption keys. Because of their increased security, recent image and video encryption algorithms frequently use them.

[63] presents application of memristor, a nonlinear device possessing memory characteristics, in video encryption. It can be used to create memristive oscillators, which will produce pseudo- arbitrary sequences. Figure 9 shows structure of 2D MCM (memristive cubic map) described by the following equations:

$$\begin{aligned} x_{n+1} &= \alpha(\mu x_n^3 + (1-\mu)x_n) + \beta \sin((y_n^2 - 2)x_n) \\ y_{n+1} &= 0.9x_n + y_n \end{aligned} \tag{3}$$

Where, α, β and μ are control parameters. The C program of 2D-MCM runs on STM32F407ZGT6 microcontroller. Specific regions of the video are selectively encrypted. Secret Key Space Analysis, Histogram Analysis, NPCR and UACI values and efficiency analysis proves the security capabilities of the algorithm. Comparative results of the correlation analysis present less correlation of encrypted frames as compared with previous research work.

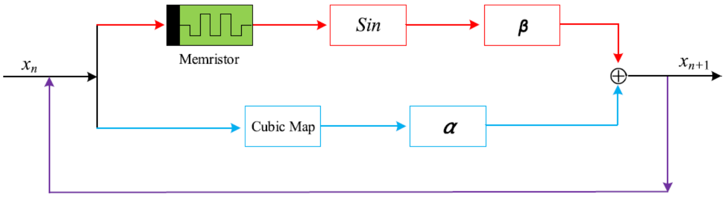

Figure 9. Structure of the 2D memristive cubic map [63]

A 2-dimensional hyperchaotic exponential adjusted Logistic and sine map (2D-HELS) is used for image encryption in [64]. The algorithm steps are the key initialization, 2D-HELS-based pixel dynamic permutation for scrambling, and dynamic RNA diffusion. The system is tested using secret key analysis, statistical analysis and differential attack test. The chaos trajectory, bifurcation diagram and Lyapunov exponent also proves robustness of the algorithm.

Selective video encryption is achieved using 2D extended Schaffer function map (2DESFM). The video extraction process is conducted using the YOLO v5. The input video is separated, annotated and the key details are extracted. Neural network weights and biases are extracted from the video using Logistic map. The secret key is dynamically produced by a neural network, with uses the critical areas of the video as inputs to the neural network. The results are compared with other image and video encryption algorithms. The results are tested on Gymnastics at the Olympic Games and public datasets and statistical results indicate improved performance over previous research. [65]

Another recent video encryption method is based on temporal action segmentation. This approach focusses crucial critical frames. It lowers the amount of resources needed for conventional frame-by-frame encryption techniques. A chaotic system known as the two-dimensional Gramacy&Lee map (2D-GLM), which performs better than other 2D maps currently in use, is developed in order to produce the key streams utilising pseudo-random sequence generation. The Georgia Tech Egocentric Activities (GTEA) dataset, which contains seven categories of everyday activities, is used for the assessments. The findings demonstrate the algorithm's high level of security and efficiency. [66]

The system using logistic map and Henon map may exhibit poor dynamic behavior in some particular parameter space. To solve this, [67] presents image encryption algorithm using 3D Improve-Henon-and-Logistic map (3D-IHAL) which provides continuous parameter space.The algorithm is implemented using MATLAB R2019a on Win10 system, I5-4210 CPU. The algorithm requires much less time (0.1471 sec for 256×256 image, 0.6114 sec for 512×512 image). So, it can be used for large-scale image encryption. But the results do not include color images.

Table 3 summarizes the implementations, specific application and types of code used for error correction. The results of the implementations are added. The result improvements as compared with earlier research and the gaps in the existing research are presented. This systematic survey will guide future researchers and reduce their efforts.

6. IMPLEMENTATION OF AES AND ENCODING METHODS FOR SATELLITE APPLICATIONS

The communication systems used in satellites in space are vulnerable to radiation and vacuum effects. So the electronic hardware exposed to these effects can cause data loss or errors in the data. The research work in this area mainly includes efforts to reduce the data loss because of the environmental effects.

The satellite communication systems are affected by radiation and vacuum effects. These effects are known as Single Event Effects (SEE). There are mainly three types of SEE: Single Event Latch-up (SEL), Single Event Upset (SEU), and Single Event Burn-out (SEB) [68]. Many researchers have worked for the development of systems for the reduction of SEE [69] [68] [70] [71].

Few researchers have implemented Crypto-Coding for satellite applications, where channel coding is utilized for bit error correction at low SNR. Different types of encoding methods are used such as hamming code [69] [72], Low-density parity-check code (LDPC) [73], and Turbo code [74] [75].

Turbo codes [76] are better suitable for power-limited satellite applications because they encode the data with low complexity at the satellite and decode it with high complexity at the receiver. In contrast, LDPC codes operate in the reverse way. Additionally, with few iterations and low coding rates, they obtain good error performance and approach to the Shannon limit in a weak-SNR situation [77].

S. Ghaznavi et. Al. [70] aimed at the mitigation of SEU and proposed error correction methods. This approach reduces hardware use, facilitates 100% single-bit SEU coverage, and gives a low failure in time. TMR software techniques are also used for protection against SEU on FPGAs [71]. But the TMR logic triplicate utilized memory resources as it uses the majority voter algorithm. These methods are only used for SEUs and not for SEL/SEB.

Clock frequency, Block RAM, Throughput, and Efficiency (Mbps/Area) of previous research work [87] [88] [89] [90] [91] [92] are compared in [93]. Better implementation efficiency is achieved than previous work. Table 4 summarizes the cryptographic primitives for satellite applications.

[68] presents implementation of algorithm based S-box architecture on XILINX SPARTAN 3E SRAM based FPGA. The results are compared with table based AES S-box implementation. Algorithm based implementation requires 1135 Configurable Logic Blocks. Table based implementation uses less CLBs, 869 but BRAM (Block RAM) will be utilized. By avoiding use of BRAM, AES will be protected from Single event effects in satellite.

In 2020, a high-throughput AES execution is presented along with its optimizations like randomization of IV and key generation algorithm [88]. Different throughput (in Gbps) values and Efficiency (Mbps/area) values are presented for different optimizations. The algorithm is implemented on Xilinx Virtex-6 FPGA and simulated using Modelsim software. Maximum throughput of 89.7 Gbps and maximum efficiency of 12.57 Mbps/area is obtained.

Table 3. Survey of research using error correction schemes

Ref. No.	Year	Applications and code used	Implementation details	Research outcomes	Enhancement in earlier research and Gaps
[78]	2008	Data transmission Code :LDPC	Secure LDPC error correcting cipher	Resistance to linear, differential and square attacks	Gap: Hardware implementation is not discussed.
[79]	2009	Wireless sensor networks Code :ML/AES-LDPCC-CPFSK	Implementation of 4CPFSK, 8CPFSK and 16CPFSK	High channel throughput and security, easy implementation	Reduction in bit error rates compared to earlier research.
[80]	2011	ZigBee Ready RF Transceiver Code :Error Correction Based Cipher	Xilinx SPARTAN 3E XC3S1200E-4FT256 FPGA	Hardware requirement reduced	Gaps: resistance to attacks not discussed
[81]	2014	Code : QC-LDPC	(2048, 1536)-QC-LDPC code	Less chances of attacks (2^{-218}).	2.2 Kbits keys. Key sizes are less than Earlier research with 2.5 Kbits.
[82]	2015	Code : AES(128 bits) with (255, 223, 4) binary BCH and QC-LDPC	MATLAB	Separate coding compared with crypto-coding schemes.	Enhanced error performance of Concatenated schemes(BER of 10-5)
[83]	2017	High-speed communications Code :POLAR	Secure channel coding with less key size (1.6 kbits)	Immune to brute force, RN and Struik-Tilburg attacks.	Key size less than [81]
[84]	2017	Resource constrained applications. Code : QC LDPC	Nonlinear crypto coding using structured LDPC	Reduced errors.	More secure, hardware reduced than [80] Gaps: high complexity implementation
[85]	2020	Band limited AWGN channels Code :AES and QC-LDPC Lattice-Codes	Coding and modulation combined with cryptographic module	Enhanced information rate, 252-bits key	Results improved as compared with [84] Gap: nonlinear functions F and F −1 increase complexity.
[86]	2020	Data transmission Code :AES +polar codes	VMware Workstation, Hadoop platform.	Parallel computing reduces time to encrypt compared to serial computing by 71%.	Resistance to Power Analysis, brute force and Square attack. superior to [73]
[53]	2021	5G Systems-reduced latency Code :AES+LDPC	MATLAB	Image recovered at SNR greater than 2 dB.	1. Faster operation as compared with [73] 2. Simple operation than [86]
[13]	2023	Code :AES+LDPC	Key sharing problem of AES is solved using neural key exchange protocol	Results verified using the SSIM and PSNR	Better than the results of [50] and [51].

Virtex-5 XC5VLX50T FPGA from Xilinx is used to implement the iterative looping architecture for remote sensing applications. The hardware implementation of the LST-SW (Land Surface Temperature Split Window) algorithm achieved 1634.71 Mbps throughput with a maximum frequency of 268.196 MHz. 6% of slice, 12% of Number of Slice Registers and 11% of Number of Slice LUTs and one block of RAM were utilized [90].

7. SECURITY STRENGTH EVALUATION PARAMETERS

The strength of implemented cryptographic algorithm against attacks can be measured using various security parameters. The mathematical values can be derived from original image, encrypted image and decrypted image. The visual analysis can be performed from histogram and correlation plots.

7.1 Histogram plots:

The intensity of pixels in a graphic is displayed through a histogram. By comparing the histograms of the two images, it is possible to see how drastically different the pixel distributions are in the original and encrypted images. The histogram values of the encrypted output should be uniform to have resistance against histogram attacks. This constant histogram makes the system more robust, more trustworthy, and more difficult for an opponent to decipher.

7.2 Information entropy:

Entropy is the statistical parameter used to assess confusion and randomness in an image. It has a maximum confusion value of 8. If I is the total count of pixels in the image, entropy can be given by

$$\mathrm{Entropy} = -\sum_{i=1}^{I} x_i \log x_i \tag{4}$$

Where, x_i is the possibility of pixel redundancy. A robust algorithm should provide encrypted image entropy value close to 8.

Table 4. Summary of research work: Implementation of AES and encoding methods for satellite applications

Ref.no.	Year	Code type/Method	Work done/Implementation	Results
[69]	2011	AES OFB +(12,8) hamming	• Analysis of propagation of SEU faults during on-board encryption	• High level of reliability
[73]	2014	AES+ LDPC	• MATLAB • Classical SPN structure in block coding area	• Improved bit error performance • Resistance to differential, saturation and power analysis attacks
[74]	2014	Turbo	• MATLAB Simulink tool	• BER of 4 × 10^{-5} at an SNR of 10 dB • 16-QAM modulator and demodulator
[72]	2015	Hamming(12,8)	• FPGA advantage 8.1 from Mentor Graphics • ModelSim 6.3a. • MATLAB for verification	• 1 bit error detection, correction • Error injected in the plaintext • Errors also injected during the encryption • Tested by applying faulty sub bytes state matrix.
[94]	2017	AES-CTR and GEFFE generator	• MATLAB	• Resistance to statistical attacks • Correlation Coefficient Analysis
[68]	2019	Algorithm based s-box architecture	• XILINX SPARTAN 3E SRAM based FPGA • XILINX ISE 12.1 • Modelsim version 6.6b • Security against SEE	• Comparison of CLBs of FPGA used for table based and algorithm based methods • Improvement in algorithms of [69] , [70] and [71].
[93]	2020	AES-CTR, Shuffling of IV and Keys before applying AES	• Xilinx Virtex-6 FPGA • Modelsim	• Resistance to Known Key, Side-channel,Nonce Misuse Attacks • Lightweight optimization with 4 rounds instead 10 • Tower field algorithm for s-box • Results of LUT and throughput compared
[95]	2020	LST-SW Algorithm with Iterative Looping Architecture	• VHDL • XILINX VIVADO 14.7 using Test Bench Waveform Generator • Virtex-5 LX50T FPGA	• Throughput of 1634.71 Mbps • 6 % of slice in area utilization with one block of RAM
[75]	2022	CFB-AES and Turbo	• Cross-Layer Encryption	• Security against brute-force and meet-in-the-middle attacks • BER improved with 12-dB coding gain

7.3 Analysis of correlation coefficients:

In image encryption, the correlation between adjacent pixels is an important parameter that demonstrates the diffusion and confusion properties. The value of a particular pixel is very close to the values of its horizontal, vertical, and diagonal adjacent pixels in plain images. Thus, correlation values will be high. The attackers can crack the cipher data using this property. So, to resist statistical attacks, adjacent pixels should be weakly linked. So, coefficient values should be close to 0. The coefficient value ranges between −1 and 1.

The correlation coefficient is calculated using

$$rxy = \frac{Cov(x,y)}{\sqrt{D(x)*D(y)}} \tag{5}$$

$$Cov(x,y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - \mathbb{E}\{x\})\,(y_i - \mathbb{E}\{y\}) \tag{6}$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - \mathbb{E}\{x\})^2 \tag{7}$$

$$D(y) = \frac{1}{N}\sum_{i=1}^{N}(y_i - \mathbb{E}\{y\})^2 \tag{8}$$

$$\mathbb{E}\{x\} = \frac{1}{N}\sum_{i=1}^{N} x_i \tag{9}$$

$$\mathbb{E}\{y\} = \frac{1}{N}\sum_{i=1}^{N} y_i \tag{10}$$

Where, x_i and y_i : values of two adjacent pixels.
N: No. of adjacent pixels of the image.
$\mathbb{E}\{x\}$ and $\mathbb{E}\{y\}$: mean value of pixels.

7.4 Analysis of inconsistency of pixels using Mean Square Error (MSE):

MSE evaluates the Avalanche effect. It indicates the ability of the algorithm to generate a substantial difference in cipher image even if a little alteration is made to the key or the input image [96].

MSE can be calculated using:

$$MSE = \frac{\sum_{i=1}^{M}\sum_{i=1}^{N}\,[Org\_img(i,j) - Cipher\_image(i,j)]^2}{M*N} \tag{11}$$

$Org\_img(i,j)$ indicates the input image pixel value at location (i, j),
$Cipher\_image(i,j)$ is the encrypted image pixel value at location (i, j).
M, N: the number of adjacent pixels in the images.

The high dissimilarity between between input and encrypted images can be proved by high values of MSE. Whereas, between input and decrypted images, MSE value should be ideally zero. Because, the correct decrypted image will be same as input.

7.5 Analysis of inconsistency of pixels using Peak Signal to Noise Ratio (PSNR)

By comparing the cipher image and its original image, PSNR evaluates the difference in pixel values. The input image will serve as the signal and the cipher image data is added as noise. PSNR is determined mathematically as [96]:

$$PSNR = 10 * \log_{10}\frac{(Max.Pixel\ value)^2}{MSE}\ (dB) \tag{12}$$

The maximum supported pixel value is generally 255. Infinite PSNR between decrypted and original images prove that the image is reconstructed properly without any loss.

7.6 Structural similarity index measure (SSIM):

SSIM compares two images based on three important parameters: contrast, luminance and structure. Its value is between 0 and 1. SSIM=1 between original and decrypted image represents similarity between both images. while for encypted image,value should be 0.

$$SSIM(x,y)=\frac{(2\mu_x\mu_y+c_1)(2\sigma_{xy}+c_2)}{(\mu_x^2+\mu_y^2+c_1)(\sigma_x^2+\sigma_y^2+c_2)} \tag{13}$$

Luminance μ_x and μ_y are calculated as:

$$\mu_y=\frac{1}{N}\sum_{i=1}^{N}y_i \tag{14}$$

Contrast values $\sigma_x \ and\ \sigma_y$ are calculated as:

$$\sigma_x=\sqrt{\frac{\sum_{i=1}^{N}(x_i-\mu_x)^2}{N-1}} \tag{15}$$

$$\sigma_{xy}=\frac{1}{N-1}\sum_{i=1}^{N}(x_i-\mu_x)(y_i-\mu_y) \tag{16}$$

$$c_1=(k_1L)^2\ ,\ c_2=(k_2L)^2 \tag{17}$$

Constants c_1 and c_2 are used to stabilize the function in the case of a null denominator. They are calculated using the default values of $k_1=0.01$ and $k_2=0.03$.

8. RESEARCH EFFORTS FOR REDUCTION OF ATTACKS

Cryptographic algorithms play an important role in communication and storage of secured information. But, encryption algorithm running on the hardware may leak sensitive information including execution time, power consumption, electromagnetic radiation and equipment fault information. Hackers may use this information to attack the system. Due to the increasing Attacks, the security of cryptographic algorithms on hardware devices has been seriously threatened.

Hamming Weight Power Model was used by Kang et al. [97] to guard against attacks on the Add Round Key stage of AES. The system is implemented using Arduino Uno. Power analysis attacks on the Arduino Uno are also analysed by Banerjee et al. [98]. The attacks on SubBytes output of AES are exploited.

[99] complements these two recent articles by illustrating the use of the differential power analysis (DPA) and correlation power analysis (CPA) techniques on the Arduino Uno microcontroller. CPA attack uses the Hamming Weight Power Model approach to create a power model of the device. On an Arduino Uno, the Add Round Key and Sub Bytes AES-128 routines are implemented. The findings demonstrate that whole 16-byte key can be determined by observing the device's power usage while performing cryptographic operations.

A Differential Fault Analysis (DFA) attack is a malicious technique that exploits a device's physical weaknesses. By intentionally introducing errors or malfunctions, often using methods like lasers or overheating, attackers can uncover vulnerabilities in cryptographic systems and steal sensitive data. [100] [101]. it is essential to assess how the DFA countermeasures would affect the effectiveness of defenses against power analysis assaults [102]. A new diffusion layer MixColumn-Plus is added to the original AES, to raise the resistance against such attacks. 2^{116} exhaustive key searches will be needed to break the security [103].

Table 5. Research Summary: Implementations for prevention against attacks

Ref. No.	Brute force attack	Cipher text only attack	Chosen plaintext attack	Chosen cipher text attack	Power analysis attack	Saturation attack	Statistical attack
[43]	✓	✓	✓	✓			
[73]			✓		✓	✓	✓
[94]							✓
[93]							✓
[75]	✓		✓				
[83]	✓						
[85]			✓				
[98]					✓	✓	✓
[99]					✓	✓	✓
[103]					✓		

The techniques for defending against Power Side-Channel and Fault Injection Attacks are examined [104]. A T-box-based AES is built on FPGA. The exploitable flaws of differential fault analysis (DFA) are analysed at the bit and byte levels. For the parity bit signature generators, the fault coverage is 98.5% and 99.99%, respectively, with an area penalty of 9% and 36%, respectively. A defect coverage of 100% is offered by the Hamming code signature generator, with an area penalty of 18%. Table 5 presents the summary of research to make the algorithms secure against attacks.

9. THE CURRENT STATUS OF CRYPTO CODING SCHEMES

For securing large amounts of data in today's era, symmetric cryptography is much more appropriate. In this review work, we would like to conclude that the AES algorithm is proven to be the best algorithm in terms of security and throughput. Also, the basic process can be modified in different ways to achieve improved performance.

Since its first formal inception when NIST selected the Rijndael as the AES algorithm, research on implementations and applications of AES has evolved significantly. Much of the research work of crypto coding runs around expanding different dimensions to the initial concept of securing the data and error correction in one scheme, along with the implementation of modified algorithms, various modes of encryption, and different encoding methods. The outcomes of the research are reduction in hardware resources used, reduction in power consumption and reduction in complexity compared with other related schemes. It is clear from the results that when the size of the key increases, it needs more power and processing delay.

AES is implemented using various hardware and software platforms. Many researchers worked on modifications of basic algorithms for performance improvement. Table-based and algorithm-based implementations of s-box are compared. The algorithm can be implementend using parallel operation to achieve encryption time gain as compared with serial computing; the computing efficiency can be tested for different block sizes and key sizes. AES-256 is comparatively secure but the AES-128 is faster. The hardware implementation of the crypto coding methods include use of XILINX SPARTAN and Virtex FPGA.

Turbo codes are suitable for power-limited satellites because they encode the data with low complexity at the satellite and decode it with high complexity at the receiver. Whereas, LDPC codes operate in the reverse way. LDPC codes have a straightforward code structure and simple parity-check trellis. As LDPC codes can be decoded at high speeds, they are preferred in time constrained applications like 5G communications. LDPC coding is incorporated in several satellite communication standards like DVB-S2, where it is used to enhance signal quality and reliability. LDPC codes are proved to be more efficient on relatively large code rates like 3/4, 5/6, 7/8 than turbo codes. Turbo codes are the best solution at the lower code rates, for example, 1/6, 1/3 and 1/2. Lower code rate indicates that more redundant bits will be added in the code word to offer high reliability.

The recent and forthcoming field of data sharing is Internet of Things (IoT). The importance of developing new cryptographic algorithms and results to cover information is emphasized, taking into consideration recent exploratory work on various IoT security results [105]. The proposed methods in [106] , [107] are using lightweight cryptography to overcome security issues and choosing solutions with the least amount of overhead and implementation impact.

For crypto-coding implementations, bit error performance with specific Eb/No and code rate is compared for different types of channels such as LMS and AWGN Channels. Successful encryption of images is proved by different histogram and correlation plots of original and encrypted images. Data security is highlighted using a Correlation graph for different keys. Only the correct key gives a Correlation equal to one. The schemes also provide security against different types of attacks like linear, square, differential, saturation, power analysis attack, and Exhaustive/brute force attack.

10. RESEARCH OPPORTUNITIES AND DIRECTIONS FOR FUTURE RESEARCH

The major challenge in developing crypto coding combinations is the proper algorithmic merging of encoding and decoding within the rounds of encryption and decryption respectively. The study in [108] reviews and summarizes numerous AES attacks and concludes that executions of a specific assault are likely to improve with time due to software or internal algorithm and parameter modifications. Thus, AES can be secured using reduced number of rounds to achieve processing time gain. Outcomes of this research can be useful for researchers to reduce processing time.

AES has lower PSNR values, is resistant to statistical attacks, and exhibits a greater disparity betwee n the input and encrypted image histograms. As the hybrid chaotic maps have greater Number of Pixels Change Rate (NPCR) and Unified Average Changing Intensity (UACI) values, they are more resistant to targeted plain text attacks or differential attacks [109]. As both the methods offer benefits against multiple types of attacks, the future research should focus on combining chaotic schemes in Block encryption.

The researchers achieved improved performance by modifying the basic AES algorithm. To achieve high security, methods like the use of more no. of keys or algorithmic implementation of s-box are proposed. But these methods make the system much more complex. The requirement for hardware resources will also be increased. One direction of research can be towards the schemes providing data security without much increase in complexity. A nonlinear function with linear complexity can be developed.

Many applications are having hardware constraints. But the use of crypto-coding for IoT is not evolved much. So crypto-coding implementations involving reduced hardware resources will be needed in the future for advancements in applications like IoT. One of the criteria for evaluation of new algorithms for NIST invited proposals was low power consumption. Implementing AES using EDK (embedded development kit) provide good results. The application of AES-New Instructions (NI) provided 13.5 time speed gain and 90% energy saving [49]. It is also used recently to design universal hash functions based on AES round functions and 128-bit XORs [110] . The implementation advantages of AES-NI can be exploited in crypto-coding field for IoT applications.

For power-limited satellite communications, Turbo codes and LDPC codes can be employed in accordance with each other. These codes can be enhanced in the future to create a crypto coding technique for power-restricted applications. Quasi-Cyclic LDPC code offers faster decoding and low complexity. So, it can be used for high speed requirements such as 5G. The crypto coding system can be designed using Quasi-Cyclic LDPC codes and AES on various platforms and the result can be compared to derive best-suited hardware platform. Also for high speed encryption, compression and then encryption can be used. The future research can be based on efficient encryption of audio and video as well.

11. CONCLUSION

The security, speed, and hardware complexity of traditional cryptographic systems are improved using crypto-coding methods. Encryption algorithms are compared initially in the presented survey based on implementation outcomes. With little use of hardware resources, AES offers the highest security strength and greatest throughput for encrypting large volumes of data. Also, modifications may be made to the core algorithm for better performance.

The crypto-coding based on different encoding types, like Hamming, Polar, Low-density parity-check code, and Turbo code is explored. Since LDPC code has good error performance, it is most frequently employed in crypto-coding. It gets employed for high-speed requirements like 5G and 6G since it provides quicker decoding. Turbo codes are more appropriate for power-constrained satellite applications to reduce the consequences of single event effects. Rather than implementing a table-based S-box design, the crypto-coding for satellite communication uses an algorithm-based S-box architecture. The key size of the cryptographic algorithm is application-dependent as larger keys need more processing and a longer delay. Thus, while AES-128 is quicker, AES-256 is more secure. Modelsim and MATLAB software are utilized for the software implementation of crypto-coding systems. FPGA boards with XILINX-ISE software facilitate the development of the encryption systems. Significant speed gains and energy savings are offered by AES-New Instructions (NI). The security is verified using mathematical and visual analysis parameters like entropy, correlation, histograms, SSIM and PSNR. Compared to other cryptographic techniques like chaotic encryption, AES has a lower PSNR, is more resilient to statistical attacks, and shows a larger difference between the input and encrypted image histograms.

Improper key management, improper initialization vectors, and poor cryptographic practices may substantially decrease the security of AES-based crypto-coding. The limitations of AES-based crypto-coding are also related to potential implementation vulnerabilities, which can reduce resistance to side-channel attacks.

The literature is categorized, and examined based on design, applications, encoding method, and security against different types of attacks. Finally, directions for future research in the area of crypto-coding are offered. The authors believe that the presented survey can fill research gaps for developers. From the perspective of the presented survey, the authors plan to develop robust cryptographic algorithms combining chaotic techniques with AES and error correction codes.

REFERENCES

[1] F. Mousa, R. Tahboub, M. Odeh, “Survey Paper: Cryptography Is The Science Of Information Security,” *International Journal of Computer Science and Security,* vol. 5, pp. 298–309, 2011.

[2] E. Mansoor , S. Khan, U. B. Khalid, “Symmetric Algorithm Survey: A Comparative Analysis,” *International Journal of Computer Applications,* vol. 61, no. 20, pp. 12-19, January 2013.

[3] N. I. o. S. a. T. (NIST), “ADVANCED ENCRYPTION STANDARD (AES),” *Federal Information Processing Standards Publication 197,* November 26 2001.

[4] J. Daemen e V. Rijmen, “The design of Rijndael : AES-the Advanced Encryption Standard,” 2002.

[5] R. f. S. D. S. Standards, “CCSDS CRYPTOGRAPHIC ALGORITHMS,” *CCSDS RECOMMENDED STANDARD FOR CRYPTOGRAPHIC ALGORITHMS*, Recommended Standard, Issue 2, August 2019.

[6] Dworkin, “Recommendation for Block Cipher Modes of Operation Methods and Techniques,” *Special Publication (NIST SP), National Institute of Standards and Technology*, 2001.

[7] E. T. S. Institute, “Digital cellular telecommunications system (Phase 2+) Channel coding (GSM 05.03),” *GSM 05.03 Version 5.1.0*, May 1996.

[8] C. G. Gheorghe, D. A. Stoichescu e R. Dragomir, “Latency requirement for 5G mobile communications,” *10th International Conference on Electronics, Computers and Artificial Intelligence*, 2018.

[9] L. Lingyun, X. Yang, J. Yueqiu, “Design and performance analysis of AES-LDPC error correcting cipher for cognitive radio systems,” *Systems Engineering and Electronics*, vol. 32, no. 1, pp. 195-199, 2010.

[10] A. Ako Muhammad , “Advanced Encryption Standard (AES) Algorithm to Encrypt and Decrypt Data,” *Cryptography and Network Security*, pp. 1-13, 2017.

[11] I. Ahmad, T. Kumar, M. Liyanage, J. Okwuibe, M. Ylianttila, A. Gurtov, “Overview of 5G security challenges and solutions,” *IEEE Communications Standards Magazine*, vol. 2, no. 1, pp. 36-43, April 2018.

[12] Bae, J., Abotabl, A., Lin, H., Song, K. e Lee, J., “An overview of channel coding for 5G NR cellular communications,” *APSIPA Transactions on Signal and Information Processing*, 2019.

[13] P. Kulkarni, R. Khanai, D. Torse, . N. Iyer, G. Bindagi, “Neural Crypto-Coding Based Approach to Enhance the Security of Images over the Untrusted Cloud Environment,” *cryptography*, vol. 7, no. 23, 2023.

[14] A. Maharaj, “A Review on Advanced Encryption Standards (AES),” January 2020.

[15] A. Hamza, B. Kumar, “A Review Paper on DES, AES, RSA Encryption Standards,” *9th International Conference System Modeling and Advancement in Research Trends (SMART)*, 2020.

[16] Ramesh, Archana, A. Suruliandi, “Performance analysis of encryption algorithms for Information Security,” *Performance analysis of encryption algorithms for Information Security*, 2013.

[17] M. Panda, “Performance analysis of encryption algorithms for security,” *International Conference on Signal Processing, Communication, Power and Embedded System (SCOPES)*, 2016.

[18] Berent, A., “Advanced Encryption Standard by Example.,” 1 April 2007. [Online]. Available: http://www.networkdls.com/Articles/AESbyExample.pdf. [Acesso 2007].

[19] Nadeem, Aamer, Mobin Javed, “A Performance Comparison of Data Encryption Algorithms,” *International Conference on Information and Communication Technologies*, 2005.

[20] Z. Hercigonja, “Comparative Analysis of Cryptographic Algorithms,” *International Journal of digital technology and economy*, vol. 1, no. 2, pp. 127-134, 2016.

[21] Diaa, S, Hatem M. A. K. Mohiy M. H., “Evaluating the Performance of Symmetric Encryption Algorithms,” *International Journal of Network Security*, vol. 10, no. 3, pp. 213-219, May 2010.

[22] R. J. Mceliece, “A public-key crypto-system based on algebraic coding theory,” *Deep Space Network Progress Report*, pp. 114–116, January and February 1978.

[23] T. R. N. Rao, “Joint encryption and error correction schemes,” *ISCA’84 Proceedings of the 11th annual international symposium on computer architecture, ACM SIGARCH computer architecture news*, New York, 1984.

[24] N. H., “Knapsack-type cryptosystems and algebraic coding theory,” vol. 15, no. 2, pp. 157-166, 1986.

[25] Struik, R. e van Tilburg, “The Rao–Nam scheme is insecure against a chosen-plaintext attack,” *Advances in cryptology—CRYPTO’87.*, vol. 293, pp. 445–457, 1988.

[26] “Private-key algebraic-code encryptions,” *IEEE Transactions on Information Theory*, vol. 35, no. 4, pp. 829–833, 1989.

[27] Hwang, T. Rao T.R.N., “Secret error-correcting codes (SECC),” *Proceedings on Advances in cryptology*, Springer, New York. , 1990.

[28] A. Oluwayomi, M. Varanasi, “Joint Scheme for Physical Layer Error Correction and Security,” *ISRN Communications and Networking*, 2011.

[29] Chai, Q. e Gong, G., “Differential cryptanalysis of two joint encryption and error correction schemes,” *Global telecommunications conference (GLOBECOM 2011) IEEE*, 2011.

[30] D. Canright, “A Very Compact S-Box for AES,” *Cryptographic Hardware and Embedded Systems – CHES 2005*, 2005.

[31] A. Satoh, S. Morioka, K. Takano, S. Munetoh, “A compact Rijndael hardware architecture with S-box optimization,” *Advances in Cryptology - ASIACRYPT 2001*, vol. 2248, Lecture Notes in Computer Science, pp. 239–254, 2001.

[32] M. B. Ghodke, S. N. Mali, “Implementation of Advanced Encryption Standard Algorithm for Communication Security Using FPGA,” *International Research Journal of Engineering and Technology (IRJET)*, vol. 3, no. 7, pp. 1176-1179, July 2016.

[33] J. Gong, W. Liu, H. Zhang, “Multiple Lookup Table-Based AES Encryption Algorithm Implementation,” *Physics Procedia*, vol. 25, 2012.

[34] Kusum Lata, Sandeep Saini, “Hardware Software Co-Simulation of an AES-128 based Data Encryption in Image Processing Systems for the Internet of Things Environment,” *IEEE International Symposium on Smart Electronic Systems (iSES) (Formerly iNiS)*, Jaipur, Rajasthan, 2020.

[35] A. A. K. A. J. Adeniyi, “Implementation of a block cipher algorithm for medical information security on cloud environment: using modified advanced encryption standard approach,” *Multimed Tools Appl,* vol. 82, pp. 20537–20551, 2023.

[36] S. S. T. &. J. A. Hussain, “Modified advanced encryption standard (MAES) based on non-associative inverse property loop.,” *Multimed Tools Appl,* vol. 82, pp. 16237–16256, 2023.

[37] S. H. B. B. S. N. M. A. E. a. H. T. E. A. Altigani, “A Polymorphic Advanced EncryptionStandard – A Novel Approach,” *IEEE Access,* vol. 9, pp. 20191-20207, 2021.

[38] E. M. De Los Reyes, A. M. Dr.Sison, R. P. Dr. Medina, “Modified AES cipher round and key schedule,” *Indonesian Journal of Electrical Engineering and Informatics (IJEEI),* vol. 7, no. 1, pp. 29-36, 2018.

[39] R. V. Kshirsagar, M. V. Vyawahare, “FPGA Implementation of High Speed VLSI Architectures for AES Algorithm,” *Fifth International Conference on Emerging Trends in Engineering and Technology*, 2012.

[40] M. Reddy e Y. Babu, “Evaluation of Microblaze and implementation of AES Algorithm using Spartan 3-E,” *International Journal of Advanced Research In Electrical, Electronics and Instrumentation Engineering.*

[41] D. Kumar, A. Reddy, J. S. A. K., “Implementation of 128-bit AES algorithm in MATLAB,” *International Journal of Engineering Trends and Technology (IJETT),* vol. 33, no. 126, 2016.

[42] D. Smékal, J. Frolka e J. Hajny, “Acceleration of AES Encryption Algorithm Using Field Programmable Gate Arrays,” *IFAC-PapersOnLine,* pp. 384-389.

[43] Meghashree B. S e B. R Sujatha, “AES based Image Encryption and Decryption using Matlab,” *INTERNATIONAL JOURNAL OF ENGINEERING RESEARCH & TECHNOLOGY (IJERT) NCESC,* vol. 6, no. 13, 2018.

[44] Y. Yuan, Y. Yang, L. Wu, X. Zhang, “A High Performance Encryption System Based on AES Algorithm with Novel Hardware Implementation,” *IEEE International Conference on Electron Devices and Solid State Circuits (EDSSC)*, 2018.

[45] Chih-Chung Lu, S.-Y. Tseng, “Integrated design of AES (Advanced Encryption Standard) encrypter and decrypter,” *IEEE International Conference on Application- Specific Systems, Architectures, and Processors*, 2002.

[46] Z. Yuan, Y. Wang, J. Li, R. Li, W. Zhao, “FPGA based optimization for masked AES implementation,” *IEEE 54th International Midwest Symposium on Circuits and Systems (MWSCAS),* 2011.

[47] Santhosh Kumar R, Shashidhar R, Mahalingaswamy A M, Praveen Kumar M S, Roopa M, “Design of High Speed AES System for Efficient Data Encryption and Decryption System using FPGA,” *International Conference on Electrical, Electronics, Communication, Computer, and Optimization Techniques (ICEECCOT)*, 2018.

[48] S. S. H. Shah, G. Raja, “FPGA implementation of chaotic based AES image encryption algorithm,” *IEEE International Conference on Signal and Image Processing Applications (ICSIPA),* 2015.

[49] E. G. AbdAllah, Yu Rang Kuang, C. Huang, “Advanced Encryption Standard New Instructions (AES-NI) Analysis: Security, Performance, and Power Consumption,” em *Proceedings of the 2020 12th International Conference on Computer and Automation Engineering (ICCAE 2020),* Association for Computing Machinery, New York, NY, USA, 2020.

[50] K. Saraf, P. Malathi, “Security enhancement of cyber-physical system using modified encryption AESGNRSA technique,” *Indonesian Journal of Electrical Engineering and Computer Science,* vol. 33, no. 2, pp. 1177-1185, 2024.

[51] E. Pisek, S. Abu-Surra, R. Taori, J. Dunham, J. Dunham, “Enhanced Cryptcoding: Joint Security and Advanced Dual-Step Quasi-Cyclic LDPC Coding,” *2015 IEEE Global Communications Conference (GLOBECOM)*, 2015.

[52] H. V. Gamido, A. M. Sison, R. P. Medina, “Implementation of Modified AES as Image Encryption Scheme,” *Indonesian Journal of Electrical Engineering and Informatics (IJEEI),* vol. 6, no. 3, pp. 301-308, 2018.

[53] L. Coulibaly, F. Ouallouche, V. Oduol, “Joint Cryptography and Channel-Coding Based on Low-Density Parity-Check Codes and Advanced Encryption Standard for 5G Systems.,” *International Journal of Electrical and Electronic Engineering & Telecommunications,* pp. 397-406, 2021.

[54] N. S. Foundation, “Report of the Working Group on Cryptology and Coding Theory,” *National Science Foundation,* April 1997.

[55] S. Raja, “ Joint medical image compression–encryption in the cloud using multiscale transform-based image compression,” *Sadhana,* vol. 44, no. 28, 2019.

[56] B. Mondal, T. Mandal, “A light weight secure image encryption scheme based on chaos & DNA computing,” *J. King Saud Univ.Comput. Inf. Sci.,* vol. 29, pp. 499–504, 2017.

[57] R. V. Chothe, S. P. Ugale, D. M. Chandwadkar, S. V. Shelke, “A Combined Cryptography and Error Correction System based on Enhanced AES and LDPC,” *7th IEEE International Conference On Computing, Communication, Control And Automation (ICCUBEA)*, Pune, India, 2023.

[58] P. S. JosephNg, Z. C. EricMok, K. Y. Phan, “Mitigating Social Media Cybercrime Revolutionising with AES

Encryption and Generative AI," *Journal of Advanced Research in Applied Sciences and Engineering Technology,* vol. 46, no. 2, pp. 124-154, 2024.

[59] Qian Mao, Chuan Qin, "A Novel Turbo-Based Encryption Scheme Using Dynamic Puncture Mechanism," *Journal of Networks,* vol. 7, no. 2, February 2012.

[60] W. Wu, Y. Yang, Z. Shi, "A Combined Encryption and Error-Correcting Scheme Based on Turbo Codes," *2013 3rd International Conference on Computer Science and Network Technology,* Dalian, China, 2013.

[61] Jie Liu, X. Tong, Y. Liu, M. Zhang , "A joint encryption and error correction scheme based on chaos and LDPC," *Nonlinear Dynamics,* pp. 1149–1163, April 2018.

[62] Manjula, "A Secure Framework For Medical Image Encryption Using Enhanced AES Algorithm," *INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH* , vol. 9, no. 2, pp. 3837-3841, February 2020.

[63] S. Gao, H. Ho-Ching Iu, M. Wang, D. Jiang, A. A. Abd El-Latif, R. Wu, "Design, Hardware Implementation, and Application in Video Encryption of the 2-D Memristive Cubic Map," *IEEE Internet of Things Journal,* vol. 11, no. 12, pp. 21807-21815, June 2024.

[64] M. Wang, X. Fu, L. Teng, X. Yan, Z. Xia, P. Liu, "A new 2D-HELS hyperchaotic map and its application on image encryption using RNA operation and dynamic confusion," *Chaos, Solitons & Fractals,* vol. 183, 2024.

[65] S. Gao, J. Liu, H. Ho-Ching Iu, U. Erkan, S. Zhou, R. Wu, X. Tang, "Development of a video encryption algorithm for critical areas using 2D extended Schaffer function map and neural networks," *Applied Mathematical Modelling,* vol. 134, pp. 520-537, 2024.

[66] S. Gao, H. Ho-Ching Iu, J. Mou, U. Erkan, J. Liu, R. Wu, X. Tang, "Temporal action segmentation for video encryption," *Chaos, Solitons & Fractals,* vol. 183, 2024.

[67] S. Gao, S. Liu, X. Wang, R. Wu, J. Wang, Q. Li, X. Tang, "New image encryption algorithm based on hyperchaotic 3D-IHAL and a hybrid cryptosystem," *Applied Intelligence,* vol. 53, pp. 27826–27843, November 2023.

[68] S. J. Hussain Pirzada, A. Murtaza, L. Jianwei, Tongge Xu, "The AES Implementation for Avoiding Single Event Effects for Satellite Application," *IEEE 9th International Conference on Electronics Information and Emergency Communication (ICEIEC),* 2019.

[69] C. J. N. Cheltha, R. Velayutham, "A novel error-tolerant method in AES for satellite images," *International Conference on Emerging Trends in Electrical and Computer Technology,* 2011.

[70] S. Ghaznavi, C. Gebotys, "A SEU-resistant, FPGA-based implementation of the substitution transformation in AES for security on satellites," *10th International Workshop on Signal Processing for Space Communications,* 2008.

[71] Y. Jiang, J. Han, X. Zhu e M. Cai, "Single event upset mitigation testing of SRAM-based FPGAs," *Journal of Beijing University of Aeronautics and Astronautics,* vol. 40, pp. 1073-1077, 2014.

[72] S. Mohamed, K.A. Shehata, Hanady Issa, "FPGA implementation of a combined hamming AES error tolerant algorithm for on board satellite," *World Congress on Information Technology and Computer Applications Congress (WCITCA),* 2015.

[73] Li Ning, Lin Kanfeng, Wenliang Lin, D. Zhongliang, "A Joint Encryption and Error Correction Method Used in Satellite Communications," *China Communications,* vol. 11, no. 3, pp. 70-79, 2014.

[74] R. Khanai, G. H. Kulkarni, D. A. Torse, "AES-TURBO as a single primitive for land mobile satellite channel," *IEEE Students' Conference on Electrical, Electronics and Computer Science,* 2014.

[75] S. Jeon, J. Kwak, J. P. Choi, "Cross-Layer Encryption of CFB-AES-TURBO for Advanced Satellite Data Transmission Security," *IEEE Transactions on Aerospace and Electronic Systems,* vol. 58, pp. 2192-2205.

[76] C. Berrou, A. Glavieux, P. Thitimajshima, "Near Shannon limit error-correcting coding and decoding: Turbo-codes," *Proceedings of ICC '93 - IEEE International Conference on Communications,* 1993.

[77] Brejza, Matthew F, Liang, Maunder, "20 years of turbo coding and energy-aware design guidelines for energy-constrained wireless applications," *IEEE Communications Surveys & Tutorials,* vol. 18, no. 1, pp. 8-28, 2015.

[78] Qing Su, Yang Xiao, "Design of LDPC-based error correcting cipher," *IET 2nd International Conference on Wireless, Mobile and Multimedia Networks (ICWMMN 2008),* 2008.

[79] Hakan Cam, O. N. Ucan, N. Odabasioglu, A. C. Sonmez, "Performance of joint multilevel/AES-LDPCC-CPFSK schemes over wireless sensor networks," *International journal of communication systems,* vol. 23, no. 1, pp. 77-90, January 2010.

[80] O. Adamo, M. R. Varanasi, "Joint Scheme for Physical Layer Error Correction and Security," *International Scholarly Research Notices,* vol. 2011, 2011.

[81] M. Dakhilalian, M. Esmaeili, T. A. Gulliver, "New secure channel coding scheme based on randomly punctured quasi-cyclic-low density parity check codes," *IET Communications,* vol. 8, no. 14, pp. 2556-2562, 2014.

[82] K. Viswanath, P. V. Pearlsy, "Cryptocoding system based on AES and concatenated coding scheme involving BCH and QC-LDPC," *2015 International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT),* 2015.

[83] B. Mafakheri , T. Eghlidos, H. Pilaram, “An efficient secure channel coding scheme based on polar codes,” *The ISC International Journal of Information Security,* vol. 9, no.2, pp. 111-118, July 2017.

[84] C. M. Stuart, P. P. Deepthi, “Nonlinear Cryptosystem Based on QC-LDPC Codes for Enhanced Security and Reliability with Low Hardware Complexity and Reduced Key Size,” *Wireless Personal Communications volume,* vol. 96, pp. 4177–4197, 2017.

[85] K. Bagheri, T. Eghlidos, M. R. Sadeghi, D. Panario, H. Khodaiemehr, “A Joint Encryption, Channel Coding and Modulation Scheme Using QC-LDPC Lattice-Codes,” *IEEE Transactions on Communications,* vol. 68, no. 8, pp. 4673-4693, Aug 2020.

[86] D. Xiao, Z. Gu, C. Yang, N. Sun, “Data Transmission Scheme Based on AES and Polar Codes,” *International Wireless Communications and Mobile Computing (IWCMC),* 2020.

[87] B. Dhaou, N. gia, P. Liljeberg, H. Tenhunen, “Low-Latency Hardware Architecture for Cipher-Based Message Authentication Code,” *50th International Symposium of Circuits and Systems ISCAS 2017*, Baltimore, MaryLand, USA, 2017.

[88] J. C. Resende, R. Chaves, “Compact dual block AES core on FPGA for CCM Protocol,” *25th International Conference on Field Programmable Logic and Applications (FPL)*, 2015.

[89] Y. Wang, Y. Ha, “High throughput and resource efficient AES encryption/decryption for SANs,” *IEEE International Symposium on Circuits and Systems (ISCAS),* 2016.

[90] S. J. H. Pirzada, A. Murtaza, L. Jianwei, T. Xu, “The Parallel CMAC Authenticated Encryption Algorithm for Satellite Communication,” *IEEE 9th International Conference on Electronics Information and Emergency Communication (ICEIEC),* 2019.

[91] S. Koteshwara, A. Das, K. K. Parhi, “Architecture Optimization and Performance Comparison of Nonce-Misuse-Resistant Authenticated Encryption Algorithms,” *IEEE Transactions on Very Large Scale Integration (VLSI) Systems,* vol. 27, no. 5, pp. 1053-1066, May 2019.

[92] S. Koteshwara, A. Das, K. K. Parhi, “Performance comparison of AES-GCM-SIV and AES-GCM algorithms for authenticated encryption on FPGA platforms,” *2017 51st Asilomar Conference on Signals, Systems, and Computers*, 2017.

[93] S. J. H. Pirzada, M. N. Hasan, Z. W. Memon, M. Haris, L. Jianwei, “High-Throughput Optimizations of AES Algorithm for Satellites,” *2020 International Symposium on Recent Advances in Electrical Engineering & Computer Sciences (RAEE & CS)*, 2020.

[94] E.H. Bensikaddour, Youcef Bentoutou, N. Taleb, “Satellite image encryption method based on AES-CTR algorithm and GEFFE generator,” *8th International Conference on Recent Advances in Space Technologies (RAST),* 2017.

[95] A. E. Makhloufi, N. Tagmouti, N. Chekroun, S. E. Adib, J. A. Sobrino, N. Raissouni, “AES/FPGA Encryption Module Integration for Satellite Remote Sensing Systems: LST-SW case,” *3rd International Conference on Advanced Communication Technologies and Networking (CommNet),* 2020.

[96] A. C. B. H. R. S. E. P. S. W. Zhou, “Image quality assessment: from error visibility to structural similarity,” *IEEE Trans. on Image Proc,* pp. 600-612, 2004.

[97] Y. J. Kang, T. Y. Kim, J. B. Jo, H. J. Lee, “An Experimental CPA attack for Arduino Cryptographic Module and Analysis in Software-based CPA Countermeasures,” *International Journal of Security and Its Applications,* vol. 8, no. 2, pp. 261-270, March 2014.

[98] U. Banerjee, L. Ho, S. Koppula, “Power-Based Side-Channel Attack for AES Key Extraction on the ATMega328 Microcontroller,” *Journal of cyber Security Technology,* December 2015.

[99] O. Lo, W. J. Buchanan, D. Carson, “Power analysis attacks on the AES-128 S-box using differential power analysis (DPA) and correlation power analysis (CPA),” *Journal of Cyber Security Technology,* vol. 1, no. 2, pp. 88-107, 2017.

[100] S. Patranabis, J. Breier, D. Mukhopadhyay, S. Bhasin, “One Plus One is More than Two: A Practical Combination of Power and Fault Analysis Attacks on PRESENT and PRESENT-Like Block Ciphers,” *2017 Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC),* 2017.

[101] A. Chakraborty, B. Mazumdar, D. Mukhopadhyay, “A Combined Power and Fault Analysis Attack on Protected Grain Family of Stream Ciphers,” *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems,* vol. 36, no. 12, pp. 1968-1977, December 2017.

[102] F. Regazzoni, L. Breveglieri, P. Ienne, I. Koren , “Interaction Between Fault Attack Countermeasures and the Resistance Against Power Analysis Attacks,” *Fault Analysis in Cryptography,Part of the Information Security and Cryptography book series (ISC),* pp. 257–272, 2012.

[103] A. S. A. &. C. D. Ghosal, “ Differential fault analysis attack-tolerant hardware implementation of AES,” *The Journal of Supercomputing,* vol. 80, pp. 4648–4681, 2024.

[104] Z. Kazemi, M. Fazeli, D. Hely, V. Beroulle, “Hardware Security Vulnerability Assessment to Identify the Potential Risks in A Critical Embedded Application,” *2020 IEEE 26th International Symposium on On-Line Testing and Robust System Design (IOLTS)*, 2020.

[105] I. K. Dutta, B. Ghosh, M. Bayoumi, “Lightweight Cryptography for Internet of Insecure Things: A Survey,” *2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC)*, 2019.

[106] N. A. Gunathilake, A. Al-Dubai, W. J. Buchana, “Recent Advances and Trends in Lightweight Cryptography for IoT Security,” *2020 16th IEEE International Conference on Network and Service Management (CNSM)*, Izmir, Turkey, 2020.

[107] D. Sumit, B. Singh, P. Jindal, “Lightweight Cryptography: A Solution to Secure IoT,” *Wireless Personal Communications*, vol. 112, no. 4, pp. 1-34, 2020.

[108] J.P. Aumasson, “Too Much Crypto,” *Cryptology ePrint Archive preprint, Report 2019/1492.*

[109] N. Chaudhary, T. Shahi, A. Neupane, “Secure Image Encryption Using Chaotic, Hybrid Chaotic and Block Cipher Approach,” *Journal of Imaging*, vol. 8, no. 167, 2022.

[110] A. Bariant, J. Baudrin e G. Leurent, “Fast AES-Based Universal Hash Functions and MACs,” *IACR Transactions on Symmetric Cryptology*, vol. 2024, no. 2, pp. 35–67, 2024.

BIOGRAPHIES OF AUTHORS

Rupaliben V Chothe is working as an Assistant Professor in Electronics and Telecommunication Engineering department of K. K. Wagh Institute of engineering Education and research, Nashik, Maharashtra since last 16 years. She is pursuing Ph.D. in Electronics and Telecommunication from Savitribai Phule Pune University. She can be contacted at email: rvchothe@kkwagh.edu.in

Dr Sunita P Ugale is working as a Professor in Electronics and Telecommunication Engineering department of K. K. Wagh Institute of engineering Education and research, Nashik, Maharashtra since last 28 years. She holds Ph.D. degree and her special fields of interest include Fiber Optics Communication, Optical Sensors, Automation and VLSI technology. She can be contacted at email: spugale@kkwagh.edu.in

Dr Dinesh M Chandwadkar is a Professor and head of E & TC Department at K. K. Wagh Institute of Engineering Education & Research, Nashik, India. His area of interest includes Signal Processing, Power Electronics, Mechatronics, and Automotive Electronics etc. He holds Ph.D. degree and he has published More than 50 research papers in reputed Journals. He is working as Board of Studies member of Electronics and Telecommunication Engineering for Pune University. He can be contacted at email: dmchandwadkar@kkwagh.edu.in

Shraddha V Shelke is working as an Assistant Professor in Electronics and Telecommunication Engineering department of K. K. Wagh Institute of engineering Education and research, Nashik. She is perusing her Ph. D. in Electronics and Telecommunication from Savitribai Phule Pune University. She can be contacted at email: svshelke@kkwagh.edu.in