Joint Cryptography and Channel-Coding Based on Low-Density Parity-Check Codes and Advanced Encryption Standard for 5G Systems

Lasseni Coulibaly[1], Fethi Ouallouche[2], and Vitalice Oduol[3]
[1] Pan African University Institute for Basic Sciences, Technology and Innovation (PAUSTI) hosted at Jomo Kenyatta University of Agriculture and Technology (JKUAT)/Electrical Engineering (Telecom), Nairobi, Kenya
[2] Mouloud Mammeri University of Tizi-Ouzou (UMMTO)/Electronics, Tizi-Ouzou, Algeria
[3] University of Nairobi (UoN)/ Electrical and Information Engineering, Nairobi, Kenya
Email: coulibaly.lasseni@students.jkuat.ac.ke; fethi.ouallouche@ummto.dz; vitalice.oduol@gmail.com

***Abstract*—Security and reliability issues have always been a big challenge in digital communications. With the emerging 5G technologies, new requirements are introduced where latency reduction is one of the most important. In this paper, a joint security and reliability method is proposed to fulfil both requirements in a single step with reduced computational complexity that leads to reduced latency for 5G communication systems. Based on Advanced Encryption Standard (AES) cryptosystem and Low-Density Parity-Check (LDPC) codes, the proposed method processes encryption and encoding at the same time. MATLAB simulation results show that the proposed method performs better compared to the previous conventional methods where encoding is done after encryption.**

***Index Terms*—Latency, AES, LDPC, low complexity, 5G communication systems**

I. Introduction

Digital communications have experienced a lot of changes in recent decades from 2G to 4G. The fast-growing demands of communication technologies introduced new requirements to be addressed by the emerging 5G [1]. 5G is mainly about three scenarios including ultra-reliable and low latency communication (URLLC), enhanced mobile broadband (eMBB), and massive machine-type communication (mMTC) which allows a large range of applications such as the internet of things (IoT), traffic control and protection, critical industrial and infrastructure applications, and very high-speed data delivery up to 1Gbit/s [1], [2]. However, these new applications require many changes where reduced latency is one of the most important. Latency is caused by the propagation and switching delays, and the computational complexity of the systems [3]. Therefore, the design of low-complexity systems is an attractive research area for 5G latency requirements.

Manuscript received March 25, 2021; revised May 26, 2021; accepted May 30, 2021.
Corresponding author: Lasseni Coulibaly (email: coulibaly.lasseni @students.jkuat.ac.ke).

In conventional communication systems, the mechanisms are designed separately as illustrated in Fig. *1*. In this system, each mechanism represents a computational complexity that leads to higher processing time delay and then introduces additional latency in the communication. To address this issue, we propose a joint encryption and error correction method that provides security and reliability requirements in a single system as illustrated in Fig. 2.

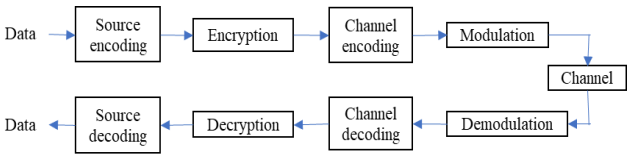


Fig. 1. Conventional communication system's structure.

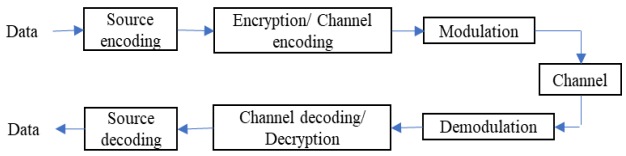


Fig. 2. Proposed communication system's structure.

In digital communication systems, data security and reliability problems have always been a big concern. Therefore, providing security and reliability of transmitted data in a single system with reduced computational complexity can contribute to solving the 5G latency requirements. To meet 5G reliability requirements, some coding techniques have been proposed such as LDPC, Turbo, and Polar codes [4]. Unlike other codes, LDPC codes benefit from faster decoding, low implementation complexity, and good error performance in high data size communications [5]. In many applications, encryption algorithms are used to ensure data security such as DES, RSA, AES, etc. [6], [7]. In most current applications where high security is required, AES is more used due to its higher security level as compared to the other cryptosystems [8]. Based on this, AES is a perfect candidate for 5G security requirements [9]. Therefore, a combined method of LDPC codes and Advanced Encryption Standard (AES) cryptosystem is the key interest of this paper.

doi: 10.18178/ijeetc.10.6.397-406

II. Literature

A. Overview of AES Algorithm

The purpose of encryption is to hide the content of data from unauthorized users [10], [11]. AES is a block cypher encryption algorithm that was proposed in the early 2000s [12], [13] to replace Data Encryption Standard (DES) for enhanced data security. Its input data called "plaintext" has a fixed length of 16 bytes (128-bits) and supports different encryption keys of length 128-bits, 192-bits, and 256-bits.

The plaintext is converted into ciphertext using a key and a non-linear mapping called the S-Box [13]. After adding the key to the plaintext, the encryption process operates four transformations such as SubByte, ShiftRow, MixColumn, and AddRoundKey in each *Nr-1* round while the MixColumn block is cancelled in the last round *Nr* [8]. For AES-128 bits, the number of rounds is *Nr = 10* (12 for AES-192 and 14 for AES-256), and the initial encryption key is expended into subkeys corresponding to each round [13]. The AES decryption process is the inverse of the encryption as shown in Fig. 3 below:

1) SubByte

After adding with the original key, the data enters the substitution block where each byte is replaced by a corresponding byte value in the S-BOX as shown in Fig. 4.

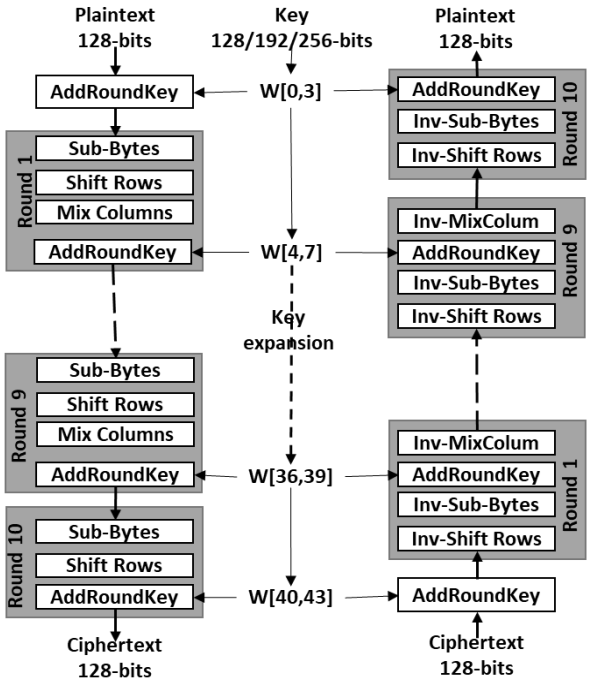


Fig. 3. AES basic encryption and decryption structure.

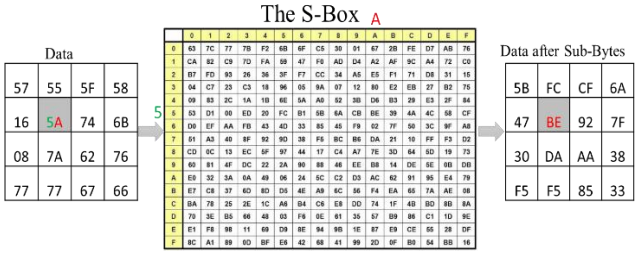


Fig. 4. Substitute byte transformation.

2) ShiftRow

The last three rows of the data in Fig. 5 are circularly shifted with 1, 2, and 3 steps respectively

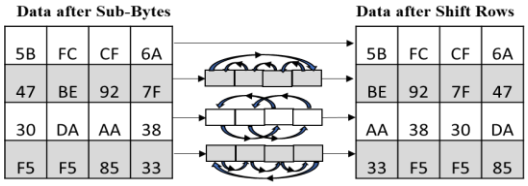


Fig. 5. Shift Rows Transformation.

3) Mix columns

Here the columns of the data are multiplied with a matrix function as shown in Fig. 6.

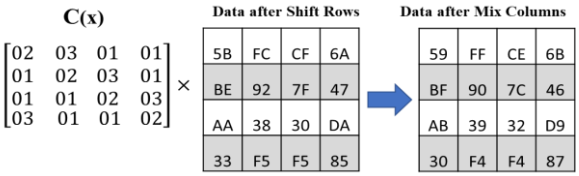


Fig. 6. Mix Columns Transformation.

4) AddRoundKey

Here the corresponding round key is added to the data with an XOR operation before the next round starts as shown in Fig. 7.

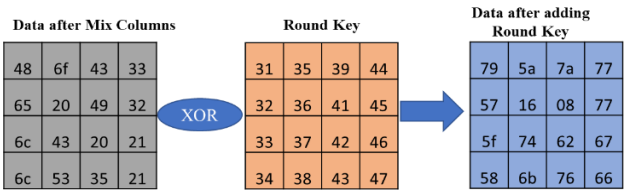


Fig. 7. AddRoundKey Transformation.

B. Key Generation and Expansion

In the AES structure, a single key is generated for encryption and decryption. This initial key is then expanded into sub-keys column by column for each round where each column is a word of 4 bytes array. In AES-128 bits, the original key of 4 words (w_0, w_1, w_2, w_3) is extended into 10 round keys of 44 words (w_0, w_1, ⋯, w_{43}) for the 10 rounds of encryption and decryption as shown in Fig. 8.

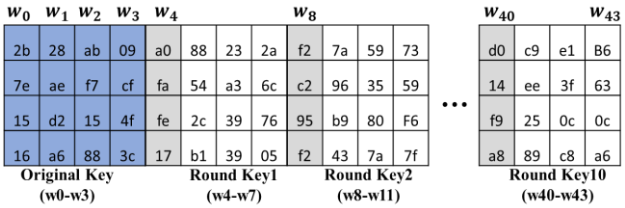


Fig. 8. The key expansion

The round keys are expanded word by word as follow:

$$K(n): w_i = w_{i-4} \oplus \text{SubByte}(\text{ShiftRow}(w_{i-1})) \oplus R_{con}(n) \quad (1)$$

$$w_i = w_{i-1} \oplus w_{i-4} \quad (2)$$

where R_{con} is the round constant vector of 4 bytes array and $\oplus$ is the XOR operator. Equation (1) derives the first word (w_4, w_8, ⋯, w_{40}) of each round key and (2) computes the other words of each round key [8].

C. Overview of LDPC Codes

LDPC codes have been initially discovered by Gallager in the early 1960s. Later, LDPC codes experienced a great rediscovery in the late 1990s where a large amount of literature is being proposed to achieve better performance close to the Shannon limit compared to its previous codes such as Turbo codes [14].

LDPC codes are linear block codes that parity-check matrix is sparse [15]. The parity check matrix **H** is formed with zeros-0 and low-density of ones-1 as shown in (3) hence their name of low-density parity-check codes. This matrix can be represented in the form of a bipartite graph called the "Tanner" graph, where columns represent "variable nodes" and rows as "check nodes" [16] as shown in Fig. 9 below:

$$\mathbf{H}=\begin{bmatrix}1&1&1&0&0&1&1&0&0&0&1&0\\1&1&1&1&1&0&0&0&0&0&0&1\\0&0&0&0&0&1&1&1&0&1&1&1\\1&0&0&1&0&0&0&1&1&1&0&1\\0&1&0&1&1&0&1&1&1&0&0&0\\0&0&1&0&1&1&0&0&1&1&1&0\end{bmatrix} \quad (3)$$

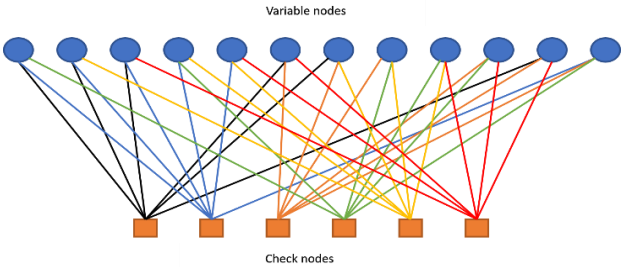


Fig. 9. Tanner graph of the LDPC code.

After the parity check matrix **H** is defined with a code rate of $R=(L-1)/L$ where L is the number of redundancy, the generator matrix **G** is derived such that the constraint $\mathbf{GH}^T=0$ is satisfied [17].

1) LDPC encoding

The encoding process is done by multiplying the message vector (**M**) and the generator matrix (**G**) then the resulting information is called the codeword (**C**) as shown in equation [16], [18].

$$\mathbf{C}=\mathbf{MG} \quad (4)$$

2) LDPC decoding

In the decoding process, a syndrome vector **S** is computed as in the following equation [16]:

$$\mathbf{S}=\mathbf{ZH}^T=[s_1, s_2, \cdots, s_{n-1}] \quad (5)$$

where **Z** is the received vector and **H** is the parity-check matrix. The received vector **Z** is a codeword (with no error) if and only if the syndrome **S = 0**. Otherwise, the received vector **Z** contains detectable errors to be corrected.

In the decoding process, two techniques are used to correct detected errors including the Bit Flipping (BF) algorithm (iterative decoding), and the Belief Propagation (BP) algorithm (sum-product decoding) [18].

D. Related Works

In 1978, McEliece was the first to propose the joint encryption and error-correcting method based on public-key encryption and the algebraic codes [19]. Later, Korzhik and Turkin claimed to broke the security of the method in 1991 [20]. After few years, many research works have been done to propose methods for improvement of the McEliece public-key system.

In 2006, Mathur, Narayan, and Subbalakshmi proposed joint high diffusion codes and the AES algorithm method [21]. The system was made to enhance the AES security but with no reduced computational complexity.

In 2008, Afshar and Aref proposed a method combining symmetric-key encryption with QC-LDPC codes [22] to achieve enhanced security level and maintain the error correction capability while the complexity of the system remains.

In 2011, Lay, Hou, and Peng proposed a joint scheme using non-homogenous LDPC codes [23]. The system could achieve good performances only within a certain range of signal-to-noise ratio which is not suitable for uncertain communication channels.

In 2014, Li *et al.* proposed in [24] a combined model of AES-128 bits with LDPC codes for satellite communication. In this method, the LDPC code is embedded in the AES last round and a new key expansion algorithm was proposed to enhance the security level. The method shows good security and reliability performances, but the computational complexity is still high since only one round of the AES is cancelled.

In 2015, Pisek, Abu-surra, Taori, Dunham, and Rajan proposed an enhanced crypto-coding method called JSALC [25]. This method claimed good Frame-Error-Rate (FER) performance by over 1.5 dB with increased security level but the computational complexity remains high.

In 2016, Hooshmand and Aref developed a combined scheme based on Latin square LDLC codes [26]. In this method, the LDLC code was used to improve the security level with an acceptable trade-off between them, but the complexity issue is unsolved.

In 2017, Khayami, Eghlidos, and Aref presented a method of quasi-cyclic-LDPC codes with finite Geometry (FG) [27] to achieve reliability and security simultaneously with lower complexity. However, the security is weak for sensitive data communications.

In 2018, Chen, Tu, and Zhang proposed to implement channel coding and encrypting in classic Turbo coding schemes [28]. It is shown that the method can both correct transmitting errors and keep information secure but with no emphasis on the complexity of the system. In [29], Liu, Tong, Liu, Zhang, and Ma proposed a joint method based on LDPC codes and a hyperchaotic system. Using the performances of the LDPC, the method aims to provide a higher security level without conflict but the computational complexity is not reduced.

In 2019, Hesam and Hashemi proposed a McEliece cryptosystem based on irregular QC-LDPC and QC-MDPC codes to reduce the key length [30]. The system

can provide reduced computational complexity, but not suitable for applications where a high-security level is required. In the same year, Jeon and Choi proposed a new joint method based on AES and Turbo codes for satellite data security and reliability [31]. The system claims to achieve better performances with processing time gains due to parallel encryption and encoding using iterations, but the computational complexity of both AES and Turbo code remain. Also, generating a new key pair for each encryption block as it is proposed, will introduce higher computational complexity for big size data transmission.

In 2020, Xiao, Gu, Yang, and Sun proposed a joint method of AES and polar code [32]. The method increased the AES security level but does not reduced enough the complexity since the Polar code just replace the ShiftRow operation in the last round of AES.

III. Proposed Joint AES-LDPC Method

Joint encryption and error correction methods described in the literature above have difficulty maintaining high security and error correction performance while reducing the computational complexity of the system. However, the proposed method in this paper can achieve both high security and good error-correcting capability with low complexity that is suitable for future communication systems where reduced latency is required such as 5G. The system's structure is shown in Fig. 10 below:

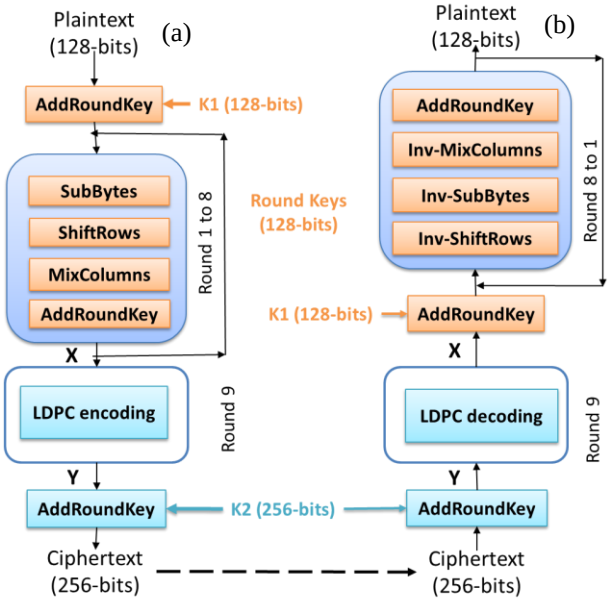


Fig. 10. The proposed AES-LDPC system' structure: a) Encryption-encoding and b) Decoding-decryption

A. AES-LDPC Encryption/Encoding

In this algorithm, the idea is to achieve the AES encryption and the LDPC encoding together to reduce the computational complexity and improve the system's performances. The AES security level is based on the following characteristics: 1) An input key of (128-bit, 192-bits, or 256-bits) that protects from plaintext attacks, 2) A nonlinear function (i.e., S-Box) that protects from differential or linear attacks, 3) And a high diffusion of 4^9 (AES-128) or above. The proposed joint AES-LDPC in this paper achieves all the above features by combining operations of AES with the LDPC code to encrypt the plaintext as illustrated in Fig. 10 (a). The encryption procedure is based on the AES (128-bits) algorithm which initially operates in 10 rounds but reduced to 8 rounds in the proposed system. The key length and the encryption block length are both 128 bits. The procedure of encryption and encoding is described by:

$$\text{Plaintext=Data (128 bits)} \tag{6}$$

$$X = \text{AES}_{1-8}^{\text{encrypt}}(\text{Plaintext}, K_1) \tag{7}$$

$$Y = \text{LDPC encoding}(X) \tag{8}$$

$$\text{Ciphertext} = Y \oplus K_2 \tag{9}$$

Equation (6) defines the input data of the proposed method. As the method combines both AES and LDPC in a single system, the input data is defined concerning the AES specifications which is a vector of 16 bytes (128 bits). The input data of the system can be text data as well as image data.

- The text data is segmented into vectors of 16 bytes (128 bits) then each vector is used as input of the system one after the other.
- For image data, the elements of the image are reorganized into vectors of 16 bytes (128 bits) then each vector is used as input of the system one after the other until the full image is encrypted-encoded. After the processes, the elements are reorganized back to the original size then show the image.

Equation (7) operates the encryption of the input plaintext based on the AES algorithm as described in the literature (A). During this operation, K_1 is used and expended into 8 subkeys for the corresponding 8 rounds.

Equation (8) operates the encoding of data based on the LDPC code. Because of the joint method, the encrypted data of 128-bits from (7) is used as the input of the LDPC code without the need to determine the code block size. During this, the parity-check matrix is generated with a code rate of R=1/2. Then, the generator matrix is derived from the parity-check matrix by using Gauss elimination and multiply it with the input vector to get the encoded data of 256-bits called a codeword.

To control the encoding process as the 9th round of the encryption algorithm, K_2 is added to the encoded data by an XOR operation and get the ciphertext at the output of the system as in (9).

B. AES-LDPC Decoding/Decryption

The decryption process shown in Fig. 10 (b) consists of the inverse of the encryption process and described by:

$$\text{Ciphertext=Data (256 bits)} \tag{10}$$

$$Y=\text{Ciphertext}\oplus K_2 \tag{11}$$

$$X=\text{LDPC decoding}(Y) \tag{12}$$

$$\text{Plaintext} = \text{AES}_{8-1}^{\text{decrypt}}(X, K_1) \tag{13}$$

Equation (10) defines the input data of the decoding-decryption process of the proposed method. Based on the

code rate R=1/2, the received vector is divided into 32-bytes (256 bits) vectors then each vector is used as input of the system one after the other until the full data is decoded-decrypted.

Equation (11) removes the security protection on the received data by adding the same K_2 using an XOR operation. Equation (12) operates the decoding of data based on the LDPC decoder. During this, the parity-check matrix is used to detect errors in the received data and the Sum-Product decoding technique is applied to recover the data.

Equation (13) operates the decryption of the data based on the AES algorithm. Because of the joint method, the decoded data of 128-bits from (12) is used as the input of the AES without the need to determine the decryption block size. During this operation, the same K_1 and its expended 8 subkeys are used in the corresponding 8 rounds of the AES decryption.

C. Key Control

A cryptosystem is considered efficient only when the encryption and decryption algorithms can be public while the key is kept secret such that, an attacker cannot be able to derive the original data without the knowledge of the encryption key. Therefore, the security of a cryptosystem is mostly based on the encryption key.

AES is a symmetric cryptosystem where the same key is used for both encryption and decryption. Based on that, the encryption key is chosen in secret by the sender and shared between the authorized users.

In the proposed joint system, two encryption keys are used such as K_1 of length 128-bits and K_2 length 256-bits. K_1 is then expanded through the standard AES key expansion algorithm for 8 rounds (w_0, w_1, ⋯, w_{35}) as shown in Fig. 8 and K_2 is used after the LDPC encoding. Since the AES algorithm and the LDPC codes are public, the security of the proposed method also depends on the secrecy of the encryption keys. Therefore, K_1 and K_2 play the most important role in the security of the system and need careful management between authorized users.

Unlike the standard AES algorithm, the use of two encryption keys in the proposed method increases the security. Even if an attacker gets one encryption key, he cannot derive the original data without the other key and the probability is very low for him to get both encryption keys through cryptanalysis attacks. Therefore, the proposed method benefits from a higher security level compared to the standard AES algorithm where only one encryption key is used.

IV. Performance Analysis

In this section, the gain of the proposed joint AES-LDPC method is shown in terms of the processing time that determine the computational complexity, the performance of security against cryptanalysis attacks, and the error correction capability. Also, numerical results are derived to show the relationships between encryption and encoding in the overall performances of the system.

A. Processing Time

As illustrated in Fig. 10, the encryption-encoding as well as the decoding-decryption operations, are activated at the same time instead of their successive activation as in conventional systems. By considering:

- $T_{\text{aes}}^{\text{en}}$ and $T_{\text{aes}}^{\text{dec}}$ as encryption time and decryption time of the AES algorithm, $T_{\text{aes}}^{\text{bs}}$ as encryption block size calculation time and M as the number of blocks.
- $T_{\text{ldpc}}^{\text{en}}$ and $T_{\text{ldpc}}^{\text{dec}}$ as encoding time and decoding time of the LDPC code with $T_{\text{ldpc}}^{\text{bs}}$ as code block size calculation time and N as the number of blocks.
- $T_{\text{aes-ldpc}}^{\text{en}}$, $T_{\text{aes-ldpc}}^{\text{dec}}$ as joint AES-LDPC encryption-encoding time and decoding-decryption time.

The processing times of the proposed method compared to the conventional method are presented in Table I where TX represents the Transmitter side and RX is the Receiver side. In the joint method, the AES algorithm operates 8 rounds instead of 10 rounds which represents a reduced complexity of 2 rounds in both side [$M \times T_{\text{aes}}^{\text{en}}(2 \text{ rounds})$ and $M \times T_{\text{aes}}^{\text{dec}}(2 \text{ rounds})$]. The LDPC code is used as the 9th round where the encrypted data is the input of the encoder without code block size ($T_{\text{ldpc}}^{\text{bs}}$) calculation. The inverse process is done in the decoding-decryption ($T_{\text{aes}}^{\text{bs}}$) part. When big data size is transmitted, the number of plaintext M increases and higher processing time gain is achieved. In literature [24], the LDPC code replace only the 10th round of AES, which achieves twice less processing time gain compared to our method. In [31], the joint AES-Turbo code claims to achieve reduced processing time based on its iterative parallel encryption and encoding but no complexity is reduced. In [32], the Polar code just replace the ShiftRow operation in the last round of AES which is less reduced complxity. Therefore, the proposed method achieves low computational complexity compared to its previous joint methods and the conventional methods that conduct encoding after encryption.

TABLE I: PROCESSING TIME AND REDUCTION GAIN

Methods	Side	Processing time	Reduced Gain
Conventional method	TX	$T_{\text{TX}} = T_{\text{aes}}^{\text{bs}} + M \times T_{\text{aes}}^{\text{en}}(10 \text{ rounds}) + T_{\text{ldpc}}^{\text{bs}} + N \times T_{\text{ldpc}}^{\text{en}}$	0
	RX	$T_{\text{RX}} = T_{\text{ldpc}}^{\text{bs}} + N \times T_{\text{ldpc}}^{\text{dec}} + T_{\text{aes}}^{\text{bs}} + M \times T_{\text{aes}}^{\text{dec}}(10 \text{ rounds})$	0
Proposed AES-LDPC method	TX	$T_{\text{TX}} = T_{\text{aes}}^{\text{bs}} + M \times T_{\text{aes-ldpc}}^{\text{en}}(9 \text{ rounds})$	$M \times T_{\text{aes}}^{\text{en}}(2 \text{ rounds}) + T_{\text{ldpc}}^{\text{bs}}$
	RX	$T_{\text{RX}} = T_{\text{ldpc}}^{\text{bs}} + M \times T_{\text{aes-ldpc}}^{\text{dec}}(9 \text{ rounds})$	$T_{\text{aes}}^{\text{bs}} + M \times T_{\text{aes}}^{\text{dec}}(2 \text{ rounds})$

B. Security Performance

The security level of the proposed AES-LDPC method is analyzed by examining its resistance to known cryptanalysis techniques as follow:

1) Resistance to differential attack

It is also called a chosen-plaintext attack where the attacker tries to deduce the encryption key by tracking the rounds and trail the difference propagation property between pairs of cipher [33]. To reach differential uniformity on a non-linear function of *n*-bits, the threshold probability is $P_d = 2^{-(n-1)}$, which has the same cryptanalysis complexity of $O(2^n)$ brute force attack. In the proposed AES-LDPC system, two different keys of size n=128 and n=256-bits are used to protect the system. An attacker needs to derive $2^{128}=3.4\times10^{38}$ and $2^{256}=1.1\times10^{77}$ possibilities to get both K_1 and K_2 which is still not possible in current days processing technologies as explained in [34]. Also, previous AES-LDPC methods as presented in the literature [24] and [25], use only one encryption key of 128-bits with an attack complexity of $2^{128}=3.4\times10^{38}$, which are more vulnerable to brute force attack compared to our proposed method. Therefore, this method offers good resistance to differential and brute force attacks.

2) Resistance to saturation or square attack

In this, an attacker tries to guess the key bytes in the 4th round of the AES algorithm using the balance changes instead of an exhaustive search in every round of AES [32]. Previous studies as indicated in [24], have shown that saturation attack can be successful on 6 rounds of AES in the complexity of $2^{63}=9.22\times10^{18}$ and that higher rounds are secure from this attack.

The proposed system uses 8 rounds of AES encryption which makes it secure from saturation attack. Additionally, the second key K_2 is not used in the AES algorithm and therefore secure from saturation attack. Also, the diffusion complexity of the proposed AES-LDPC, adds the natural diffusion of the LDPC code $d_{\min}$ with one of AES 8 rounds. $d_{\min}=16 = 4^2$ is the minimum distance of the 256-bit LDPC code. For the standard AES-128 (10 rounds), the diffusion complexity is 4^9 which goes to 4^7 when 2 rounds are cancelled. Hence, the overall diffusion of our method is $4^7\times4^2=4^9$, which maintains the diffusion complexity of the standard AES-128. Therefore, this method can resist the saturation attack the same way as AES with 10 rounds.

3) Resistance to power analysis attack

In this attack, the attacker measures the leaked energy of information in the encryption process using appropriate instruments. Then he speculates the key after the statistical analysis of power curves to decrypt the data [35]. Power analysis attack often chooses to carry out at the output moment in an AES round of encryption. Based on this, any AES algorithm using a single key as in [24] and [25] can be vulnerable because it can be attacked at the initial around which makes it easier to get the key.

Even though an attacker gets the first AES round key using this technique, the proposed method remains secure because a brute force attack will be necessary to derive the second key.

Using the LDPC coding as part of the encryption as proposed, is a reference solution to increase the system's security for future applications. Even though the LDPC generator matrix and the coding algorithm are public, unauthorized users cannot decode the information and proceed to the decryption due to the use of K_2 after encoding. Therefore, the proposed joint AES-LDPC method offers higher security compared to the standard AES algorithm.

In addition to the security performance analysis in terms of known attacks, a series of a test is done to numerically analyze the security robustness of the algorithm using the following parameters.

a) Entropy of image

The entropy of an image is a measure of disorganization, disorder and confusion. As the first objective of encryption is to hide the content of information, entropy is used to determine the level of confusion in the image data. It is calculated using the following equation [37], [38]:

$$H = -\sum_{i=1}^{n} P_i \times \log_2 P_i \tag{14}$$

where P_i is the probability of redundancy of pixels in the image, and n is the number of pixels. The maximum value of entropy is ideally 8bits/pixel.

To validate good encryption conditions, a set of images in the database as shown in Fig. 11 are used. Table II shows the results of the entropy calculation performed on the original images and their corresponding encrypted images of the database. From the results, all the values of entropy are closed to the maximum confusion value of 8. Therefore, the method can ensure good security from entropy analysis.

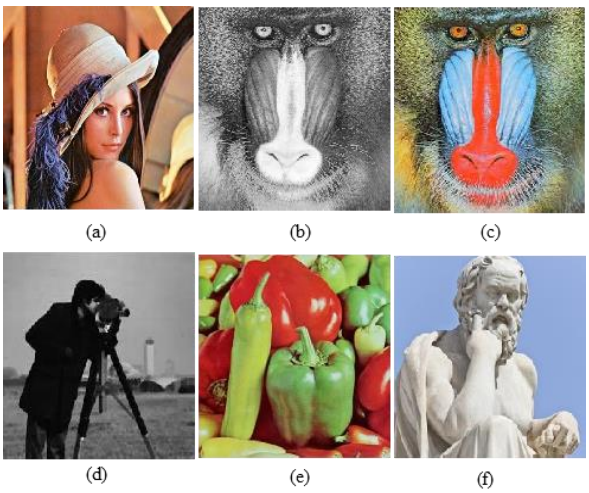


Fig. 11. Simulation images for entropy and correlation calculations.

TABLE II: ENTROPY AND CORRELATION VALUES

Images	Entropy Original image	Entropy encrypted image	Correlation
Fig.11 (a)	7.9174	7.7228	1.8051e-08
Fig.11 (b)	7.6829	7.9386	-2.8546e-08
Fig.11 (c)	7.7616	7.7245	1.2442e-08
Fig.11 (d)	7.0002	7.7198	1.2886e-07
Fig.11 (e)	7.7474	7.7194	-3.7946e-08
Fig.11 (f)	7.1974	7.7203	-7.7642e-08

b) Correlation of image

The correlation represents the strength of a relationship between two variables. This is expressed by the correlation coefficient as in the following equation [37]:

$$r_{x,y} = \text{cov}(x,y) / (\sqrt{\text{var}(x)}\sqrt{\text{var}(y)} \quad (15)$$

where $\text{cov}(x,y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y))$ is the covariance; $\text{var}(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2$ is the standard deviation; and $E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i$ is the mean. The value of the correlation coefficient range between –1.0 and 1.0. For good encryption protection, it must be negligible and very closed to zero [37].

Table II shows the correlation values obtained by comparing the original images and the encrypted images from the database in Fig. 11. The correlation results are all very closed to zero which means, the relationship between the original and the encrypted images is very small. Base on that, an attacker cannot practically find the original message from the encrypted one. Therefore, the proposed method ensures good security performance.

c) Histogram of image

The histogram of an image represents the distribution of pixels in the image according to their brightness (gray level) [36], [37]. Based on this, the histogram plots associated with the images in Fig. 12, Fig. 13 (a), and Fig. 13 (b) represent the original image, the encrypted image using the AES standard, and the encrypted image using the joint AES-LDPC method, respectively.

By comparing the histograms of the original image and the encrypted images, we can see that the distribution of pixels in the original image is hidden and not practically predictable from the distribution of pixels in the encrypted images, which means the algorithm can ensure good encryption. Moreover, the use of LDPC code in the encryption process increases two times the number of pixels in the encrypted image as shown in (b)

Fig. 13 (b) which represents two times complexity of attack. Therefore, the proposed method offers higher security compared to the AES standard algorithm from histogram analysis.

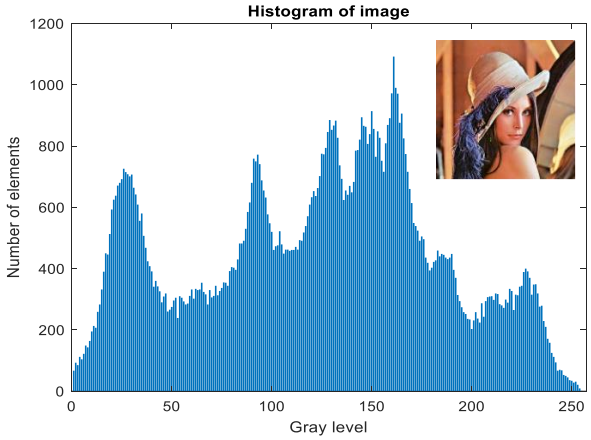
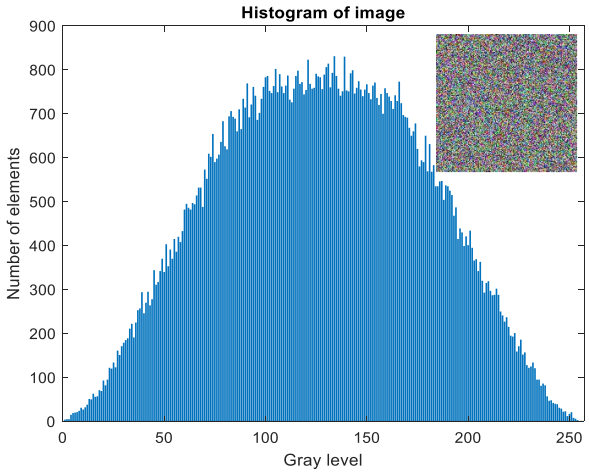
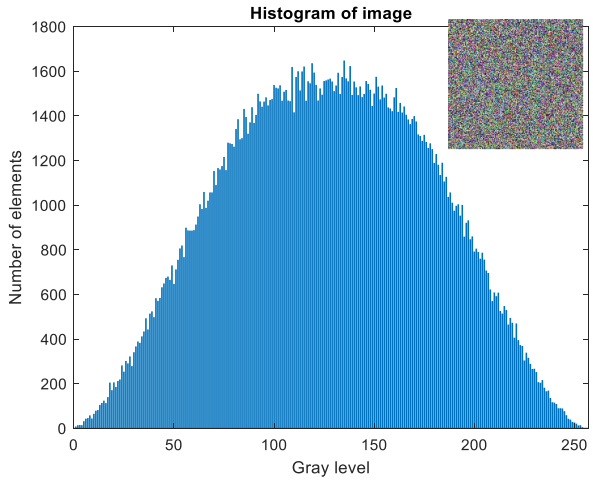


Fig. 12. Original image



(a)



(b)

Fig. 13. Encrypted Image: (a) Encrypted with the AES standard and (b) encrypted with the joint AES-LDPC method.

C. Error-Correcting Capability

This method combines AES cryptosystem and LDPC codes for the sake of reduced complexity while increasing the system's performances. This method is proposed for 5G communication systems and beyond where a large variety of LDPC codes can be applied. Based on that, the error-correcting capability of the proposed method depends on the performance of the selected LDPC code. Since the encoding and decoding processes of LDPC codes are public, the best code can be chosen to ensure the error correction performance according to different communication needs. For example, the Quasi-Cyclic LDPC codes benefit from faster decoding and low implementation complexity which is an ideal choice in a low latency communication environment as 5G. The error correction performance of the LDPC code is maintained in the proposed method while its performances are used to improve the security level with reduced computational complexity of the AES algorithm.

D. Numerical Results

To test the performances of encryption and error correction, simulations are conducted in MATLAB with the parameters in Table III.

TABLE III: SIMULATION PARAMETERS

PARAMETER	VALUE
Block length	128-bits
Key length	128 and 256-bits
Code length	256-bits
Code rate	1/2
Modulation	BPSK
Channel	AWGN
Decoding algorithm	Sum-Product
Number of Iteration	5

The code rate of the AES-LDPC encoder is R=1/2, hence the input data is arranged in blocks of 128-bits to be encrypted using the first key (K_1) and provide 256-bits encoded data. The 256-bits block is then added (XOR) with the second key (K_2) of 256-bits. After that, the data enters in the Binary Phase Shift Keying (BPSK) modulator and then sent through the Additive White Gaussian Noise (AWGN) channel. The received 256-bits data is then recovered using the inverse process.

Simulation results of the joint AES-LDPC method using image data are shown as follow. The original image in Fig. 12 is the input data of the simulation. It is encrypted using the AES standard encryption as shown in Fig. 13 (a) and then encrypted and encoded using the proposed AES-LDPC method as shown in Fig. 13 (b).

After transmission through the AWGN channel, the received image is recovered and analyzed according to the signal-to-noise-ratio (SNR) conditions of the channel. When the SNR is 0dB (Fig. 14), the image cannot be recovered due to the error diffusion effect that completely altered the signal; when SNR is 0.5dB (Fig. 15), the image can still hardly be recovered; at 1dB (Fig. 16), users are basically able to identify the image; when SNR is 1.5dB (Fig. 17), the image can be seen by users but still present some noise; when SNR is 2dB (Fig. 18), the image is recovered. However, the error-correcting performance results in Fig. 19, show that the image is completely recovered with no error when SNR is 2.5dB. With variable SNR values from 0dB to 2.5dB, the original image can get good visibility when SNR is equal to or higher than 2dB.

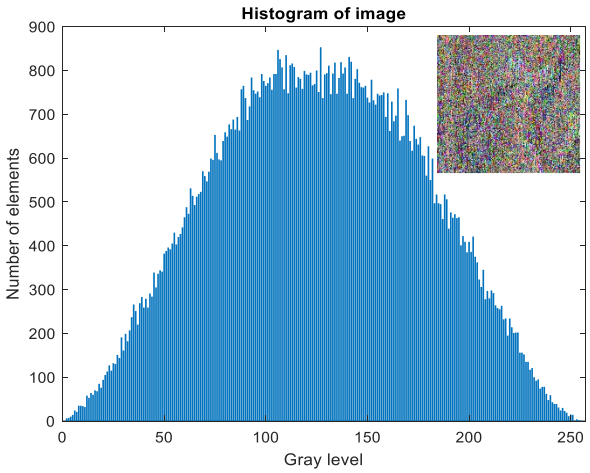


Fig. 14. Recovered image at (SNR= 0dB)

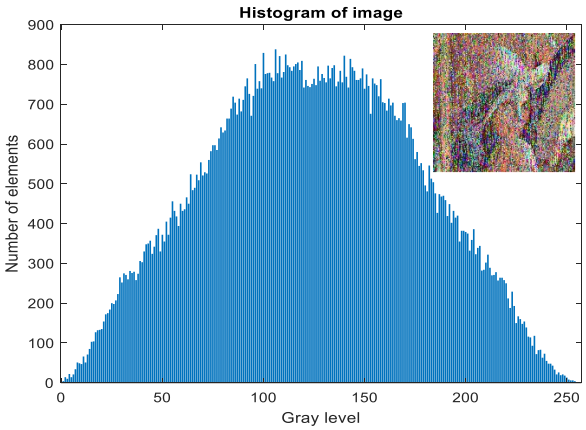


Fig. 15. Recovered image at (SNR= 0.5dB)

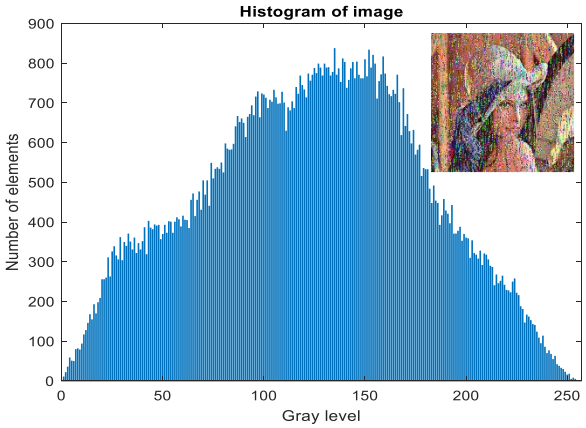


Fig. 16. Recovered image at (SNR= 1dB)

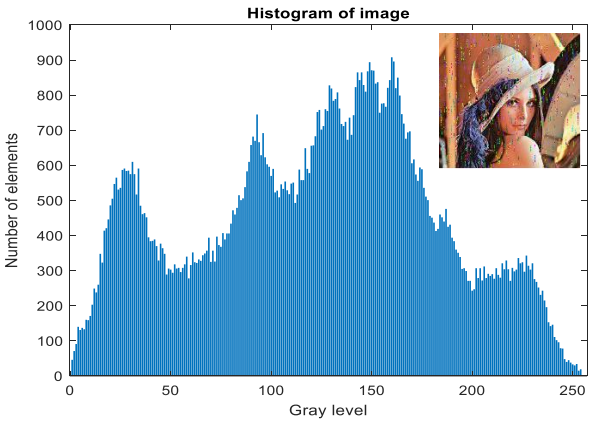


Fig. 17. Recovered image at (SNR= 1.5dB)

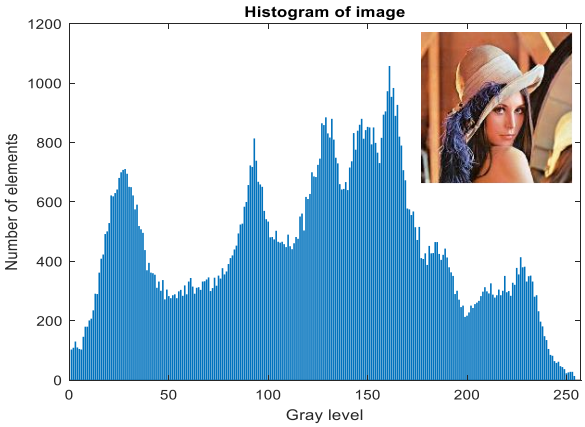


Fig. 18. Recovered image at (SNR= 2dB)

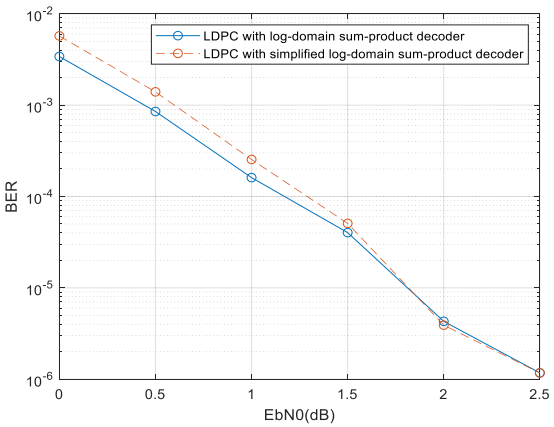


Fig. 19. The error-correcting performance

V. Conclusion

In this paper, a joint AES-LDPC method is proposed to achieve both data security and error corrections while reducing the computational complexity of the system. In the method, the LDPC code is embedded in the AES cryptosystem to replace its last two rounds, and two encryption keys are used to ensure security protection. Based on security analysis, the proposed method can resist all the well-known cryptanalysis attacks. Simulation results through the AWGN channel show that this method can accurately recover image data at SNR equal to or greater than 2dB. The error correction capability of the LDPC code is maintained in the proposed method while its performances are used to improve the security level of the AES algorithm. Due to the removed two rounds of the AES algorithm and the code block size determination cancelled in the LDPC code and their parallel activation, a high processing time gain is achieved as compared to the conventional methods. The joint method of AES and LDPC perform well with reduced computational complexity without compromising the performance of each other.

Conflict of Interest

The authors declare no conflict of interest.

Author Contributions

Lasseni COULIBALY conducted the research and wrote the paper; Fethi OUALLOUCHE supervised the work with a focus on data security with the AES encryption; Vitalice ODUOL supervised the work with a focus on the error-correction with the LDPC encoding; all authors had approved the final version.

References

[1] S. Mattisson, "An overview of 5G requirements and future wireless networks: Accommodating scaling technology," *IEEE Solid-State Circuits Magazine*, vol. 10, no. 3, pp. 54–60, 2018.

[2] Q. Xu, D. Gao, T. Li, and H. Zhang, "Low latency security function chain embedding across multiple domains," *IEEE Access*, vol. 6, pp. 14474–14484, January 2018.

[3] C. G. Gheorghe, D. A. Stoichescu, and R. Dragomir, "Latency requirement for 5G mobile communications," in *Proc. 10th International Conference on Electronics, Computers and Artificial Intelligence*, 2018.

[4] M. Sybis, K. Wesolowski, K. Jayasinghe, V. Venkatasubramanian, and V. Vukadinovic, "Channel coding for ultra-reliable low-latency communication in 5G systems," in *Proc. IEEE 84th Vehicular Technology Conference*, 2016.

[5] J. H. Bae, A. Abotabl, H. P. Lin, K. B. Song, and J. Lee, "An overview of channel coding for 5G NR cellular communications," *APSIPA Trans. Signal Inf. Process.*, vol. 8, pp. 1–14, 2019.

[6] M. Liyanage, I. Ahmad, A. B. Abro, A. Gurtov, and M. Ylianttila, *A Comprehensive Guide to 5G Security*, USA: John Wiley & Sons Ltd, 2018.

[7] S. Bhattacharya, "Cryptology and information security-past, present, and future role in society," *Int. J. Cryptogr. Inf. Secur.*, vol. 9, no. 1, pp. 13–36, 2019.

[8] A. Muhammad Abdullah, "Advanced encryption standard (AES) algorithm to encrypt and decrypt data," *Cryptogr. Netw. Secur*, pp. 1–13, 2017.

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

[10] J. Pan, P. W. Tsai, and J. Watada, *Advances in Intelligent Information Hiding and Multimedia Signal Processing*, Smart Inno. Springer, 2017.

[11] R. author Ahlswede, A. Ahlswede, I. Althöfer, C. Deppe, and U. Tamm, *Hiding Data - Selected Topics : Rudolf Ahlswede's Lectures on Information Theory 3*, Germany: Springer Nature, 2016.

[12] FIPS-197: Specification for the Advanced Encryption Standard (AES), *Fed. Inf. Process. Stand. Publ. issued by NIST*, 2001.

[13] J. Daemen and V. Rijmen, *The Design of Rijndael: AES - The Advanced Encryption Standard*. Berlin: Springer-Verlag Berlin Heidelberg GmbH, 2002.

[14] D. J. C. Mackay and R. M. Neal, "Near shannon limit performance of low density parity check codes-to be published in electronics letters," *Electron. Lett.*, vol. 33, no. 6, pp. 457–458, 1997.

[15] M. Tomlinson, C. J. Tjhai, M. A. Ambroze, M. Ahmed, and M. Jibril, *Error-Correction Coding and Decoding: Bounds, Codes, Decoders, Analysis and Applications*, Springer Nature, 2017.

[16] K. D. Rao, *Channel Coding Techniques for Wireless Communications*, Singapore Pte Ltd: Springer, 2019.

[17] K. D. Rao, "Low density parity check codes," presented at Forum for Interdisciplinary Mathematics, 2019.

[18] C. Kun, S. Qi, L. Shengkai, and P. Chengzhi, "Implementation of encoder and decoder for LDPC codes based on FPGA," *J. Syst. Eng. Electron.*, vol. 30, no. 4, pp. 642–650, 2019.

[19] R. J. McEliece, "A public-key cryptosystem based on algebraic coding theory," *The Deep Space Network Progress Report*, vol. 42, no. 44. pp. 114–116, 1978.

[20] V. I. Korzhik and A. I. Turkin, "Cryptanalysis of McEliece's public-key cryptosystem," *Lecture Notes in Computer Science*, vol. 547. pp. 68–70, 1991.

[21] C. N. Mathur, K. Narayan, and K. P. Subbalakshmi, "On the design of error-correcting ciphers," *Eurasip J. Wirel. Commun. Netw.*, pp. 1–12, 2006.

[22] A. A. S. Afshar and T. E. M. R. Aref, "Efficient secure channel coding based on quasi-cyclic low-density parity-check codes," *IET Commun.*, vol. 3, no. 2, pp. 279–292, 2008.

[23] K. Lay, C. Hou, and L. Peng, "Nonhomogeneous LDPC codes and their application to encrypted communication," in *Proc. IEEE Int. Conf. Commun.*, 2011, pp. 353–357.

[24] N. Li, K. Lin, W. Lin, and Z. Deng, "A joint encryption and error correction method used in satellite communications," *China Commun.*, vol. 11, no. 3, pp. 70–79, 2014.

[25] E. Pisek, S. Abu-surra, R. Taori, J. Dunham, and D. Rajan, "Enhanced cryptcoding: Joint security and advanced dual-step quasi-cyclic LDPC coding," in *Proc. IEEE Global Communications Conference*, 2015, pp. 2–8.

[26] R. Hooshmand and M. R. Aref, "Efficient secure channel coding scheme based on low-density Lattice codes," *IET Commun.*, vol. 10, no. 11, pp. 1365–1373, 2016.

[27] H. Khayami, T. Eghlidos, and M. R. Aref. (2017). A joint encryption-encoding scheme using QC-LDPC codes based on finite geometry. *arXiv*, 92. [Online]. Available: http://arxiv.org/abs/1711.04611

[28] D. Chen, G. Tu, and C. Zhang, "Joint channel-encryption coding based on interleaver and multiplexer in turbo codes," in *Proc. IEEE 4th Int. Conf. on Computer and Communications*, 2018, pp. 248–254.

[29] J. Liu, X. Tong, Y. Liu, M. Zhang, and J. Ma, "A joint encryption and error correction scheme based on chaos and LDPC," *Nonlinear Dyn.*, vol. 93, no. 3, pp. 1149–1163, 2018.

[30] S. Hesam and O. Hashemi, "A modified mceliece public-key cryptosystem based on irregular codes of QC-LDPC And QC-MDPC," in *Proc. 27th Iranian Conf. on Electrical Engineering*, 2019, pp. 1373–1376.

[31] S. Jeon, S. Member, J. P. Choi, and S. Member, "CFB-AES-TURBO : Joint encryption and channel coding for secure satellite data transmission," in *Proc. IEEE Int. Conf. Commun.*, 2019, pp. 1–7.

[32] D. Xiao, Z. Gu, C. Yang, and N. Sun, "Data transmission scheme based on AES and polar codes," in *Proc. Int. Wireless Communications and Mobile Computing*, 2020, pp. 172–177.

[33] D. Gérault, P. Lafourcade, M. Minier, and C. Solnon, "Revisiting AES related-key differential attacks with constraint programming," *Inf. Process. Lett.*, vol. 139, pp. 24–29, 2018.

[34] O. N. Boateng, M. Asante, and I. K. Nti, "Implementation of advanced encryption standard algorithm with key length of 256 bits for preventing data loss in an organization," *Int. J. Sci. Eng. Appl.*, vol. 6, no. 3, pp. 88–94, 2017.

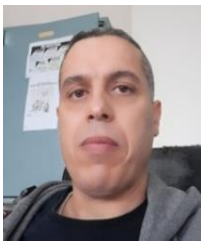
[35] O. Lo, *et al.*, "Power analysis attacks on the AES-128 S-box using Differential Power Analysis (DPA) and Correlation Power Analysis (CPA) power analysis attacks on the AES-128 S-box using," *J. Cyber Secur. Technol.*, vol. 1, no. 2, pp. 88–107, 2017.

[36] B. Xiao, H. Tang, Y. Jiang, W. Li, and G. Wang, "Brightness and contrast controllable image enhancement based on histogram specification," *Elsevier Neurocomputing*, vol. 8, no. 12, pp. 1–12, 2017.

[37] Y. Zhang, "Test and verification of AES used for image encryption," *3D Res.*, 2018.

[38] C. Cheng and S. H. I. Shen, "Efficient approach for computing the discrimination ratio-based variant of information entropy for image processing," *IEEE Access*, vol. 8, 2020.

Lasseni Coulibaly received his bachelor's degree in Electronics, and master's degree in Networks and Telecommunications from Mouloud Mammeri University of Tizi-Ouzou, Algeria in 2016 and 2018 respectively. He is currently pursuing research for a master's degree in electrical engineering (Telecommunication) at Pan African University Institute for Basic Sciences, Technology and Innovation hosted at Jomo Kenyatta University of Agriculture and Technology, Nairobi, Kenya. His research interests include data security and reliability issues, and low latency communication systems.



Fethi Ouallouche received his Magister degree in remote sensing in 2007, and his PhD degree in electronics in 2014 all from Mouloud MAMMERI University of Tizi-Ouzou (UMMTO), Algeria where he works in the faculty of electrical and information engineering/ department of electronics. He is currently a senior lecturer and a member of the analysis and modelling of random phenomena laboratory (LAMPA) in the same university. His research fields include meteorology, image processing, remote sensing, data security and telecommunications.

Vitalice Oduol received his pre-university education at Alliance High School in Kenya. Later, he received the B.Eng. (Hons.), M.Eng. and PhD. degrees in electrical engineering from McGill University, Montréal, Canada in 1985,1987, and 1992, respectively. Joined MPB Technologies, Inc. in 1989, he worked on meteor burst communication systems, satellite on-board processing, and low probability of intercept radio. In 1994 he joined INTELSAT where he did R&D work on the integration of terrestrial wireless and satellite systems. After working at COMSAT Labs. (1996-1997) on VSAT networks, and Tran Switch Corp. (1998-2002) on communication systems product definition and architecture, he joined the Department of Electrical and Information Engineering, University of Nairobi, Kenya in 2003 where he was chairman from 2006 to 2012. His research interests include performance of communication systems – analysis, modelling, simulation and evaluation. This includes signal processing, spectrum Sensing in Cognitive Radio, emerging areas (5G and beyond), Mitigation of Rain attenuation in RF signals at high frequencies. He is also interested in vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communications. Prof. Oduol is a member of IEEE and was a two-time recipient of the Douglas Tutorial Scholarship at McGill University.