Research Article

SOHAG JOURNAL OF SCIENCES

https://doi.org/10.21608/sjsci.2024.250176.1154

Medical Image Privacy Enhancement Using Key Extension of Advanced Encryption Standard

Omar Reyad*, Hanaa M. Mansour, Elnomery A. Zanaty, and Mohamed Heshmat

Computer Science Department, Faculty of Computers and Artificial Intelligence, Sohag University, Sohag 82524, Egypt.
**E-mail: oreyad@science.sohag.edu.eg*

Received: 23rd November 2023, **Revised:** 10th January 2024, **Accepted:** 15th January 2024
Published online: 17th January 2024

Abstract: In recent years, conventional encryption techniques cannot be used directly in the transmission of electronic health data. The main reason is the restrictions on data quantity, data multitude, and storage assimilation, particularly in the case that patient private data is sent through unsecured paths. Because image structure differs from textual information considering two unique elements which are damage to data and violation of confidentiality, some patients may miss out the privacy and in bad cases the integrity of owned data contents. So, an encryption scheme is required so that medical data and information can be privately shared over the Internet with other data centers without being concerned significantly about privacy breaches. This study aims at enhancing the privacy of medical images and offers protection from intrusion assaults. The proposed method makes encryption and decryption more secure and robust by using a key extension in the key schedule of the advanced encryption standard (AES) algorithm. Various safety evaluation metrics are used such as histogram, entropy, number of pixels change rate (NPCR), and correlation coefficient. The test of unified average changing intensity (UACI) is also computed. Finally, the test scores obtained show high values of the suggested medical image ciphering model is effective and convenient for health data transmission.
Keywords: Advanced Encryption Standard, Medical Image Privacy, Encryption, Decryption, Key Extension.

1. Introduction

Many industries, including digital communications, multimedia systems, medical imaging, and healthcare applications use image and video encryption methods and processes for the goal of the security of data transmission [1].

The majority of healthcare centers and hospitals have used past and modern digital communication channels and the Internet for exchanging various types of medical information, but the security of this information is not verified and cannot be granted in such open environments. With the advent of artificially intelligent and smart environments such as the Internet of Healthcare Things (IoHT), which has connected every medical thing to the Internet, medical image confidentiality and integrity have become a crucial concern in modern communication and information technology.

Smart systems and models that use multiple security algorithms can encrypt medical images for popular individuals or patients in critical situations, helping to protect patients' privacy [2].

Healthcare images come in a variety of forms, including X-ray systems, ultrasound, computed tomography (CT), magnetic resonance imaging (MRI), and positron emission tomography (PET). Each uses a different technology to generate images of the structures within the body parts. When creating a hospital information data center, the data security option is crucial [3]. Recently, there has been a lot of attention paid to the security of medical images. Typically, this involves three main aspects: confidentiality which means that only authorized people are granted access to patient data, and integrity which resists the manipulation of data during transmission and on rest. The third aspect is authentication which is involved with identification as a real-time problem. This means that the two participants setting up a communication have to recognize each other, permitting the information's origin to be assured [4].

The availability of healthcare software services around the globe enables diagnostics, data retrieval, copying, and large-scale digital imaging retrieval. It frequently leads to the fabrication of unauthorized copies or unauthorized access to vital data in the private domain [5]. Although various security measures were created and used to keep healthcare network devices out of the way of cyber-attacks, instructions about new security issues have not yet been sufficiently specified and tracked by software domain users. This implies that the end-user is unable to take preventative steps to stop such changeable data attacks. As a result, several researchers have concentrated on designing methods for imaging security in medical applications [6-8].

Encryption as a real-time example is thus one of the best techniques to secure medical image information. The data encryption standard (DES), its iteration triple DES (TDES), and the intended advanced encryption standard (AES) algorithms have all been utilized to classify the problems associated with low-level efficiency. They also take into account the small data sets and redundancy of serious cases [9]. The IoHT platform's optimal encryption for medical images is therefore ensured by these methods, which are difficult enough to handle [10]. AES is counted as one of the most widely used block ciphers in the world [11]. Despite numerous attacks, none of them have been able to completely decrypt this robust algorithm. A modification to this algorithm has been proposed to enhance the security it provides and add randomness to the original algorithm

operations.

This study's key feature is a robust encryption method with the aim of preserving the privacy of patient medical images as shown in Figure 2. The presented method took into account key extensions of 128-bits length for the suggested enhancing encryption procedure and then determined the associated image's binary value by dividing it into sixteen sub-blocks of 8-bits size. Then, it is permuted with the expansion transformation key at each round of the AES total of 10 rounds. The suggested method ensures the safeguard as well as the medical information privacy sent to healthcare facilities across multiple networks.

The next parts of this study are organized as follows. The most recent solutions described in the literature are surveyed in Section 2. An overview of the AES symmetric cipher is given in Section 3. The suggested medical image encryption and decryption methods are presented in Section 4. The performance evaluation findings and analysis are presented in Section 5. The entire work is finally concluded in Section 6.

2. Related Works

The challenge of healthcare imaging encryption has been widely discussed and studied in the most recent state-of-the-art research effort during the recent decade. To encrypt medical images and protect patient's data privacy, a variety of methods have been suggested and implemented.

A modern cryptographic technique with a significant scope of secrecy and speed is presented by the authors in [12]. For the encryption of medical images, they employ an effective variation of a hybrid system that combines elliptic curve cryptography (ECC) and the AES block cipher. The suggested approach integrates the usefulness of a symmetrical AES system for data speed and an asymmetric method of ECC for the security of the exchange of symmetric session keys. The main suggestion is to amend the AES by doing away with the mix-columns conversion and substituting an alternative permutation based on column shifts. This will reduce time complexity and at the same time keep the Shannon prevalence and the ambiguity basis intact. The algorithm of a chaotic map supported by standard encryption and investigated against AES in its original form has been developed in [13]. Researchers were able to determine the reason that chaotic maps affected encryption modality through this comparison. Instead of using regular AES encryption, the newly created technique, CAT-AES, repeatedly loops around Arnold's cat map before encrypting data. Twenty brain MRI scans and several breast cancer MRI scans were used as the two groups of 16-bits of digital imaging and communications in medicine (DICOM) images for the evaluation of both methods utilizing correlation coefficient and histogram consistency. To provide a reliable symmetric image cryptographic method, a novel modulated release of AES has been suggested in [14]. In order to address the issue of textured zones seen in other well-known encryption methods, the AES is expanded to allow a key streaming generation for image ciphering primarily for images with lower entropy values. According to a thorough assessment, the new approach provides significant security and is simple to implement in both hardware and software.

The mechanism for a hash-based bit-string generation is presented in [15]. The key impact of the suggested technique is to create bit-strings of any desired length by altering the x-value of the elliptic curve points using the provided hashing operation. Several medicinal images of major organs are encrypted using the resulting bit-string. The successful operation of the cipherimage has then been examined using numerous assessment metrics. The outcomes showed that the suggested mechanism can be applied to transmit medical images securely and privately via insecure communication networks.

In [16], a modern image cryptographic procedure based on deoxyribonucleic acid (DNA) coding and composite chaos and Qi-hyperchaos is proposed. The initial encryption in this system uses the Fibonacci transformation process and the dispersal technique of module concatenation. The final ciphertext is then calculated by DNA using the moderated ciphertext and the newly chaotic combination. The results of experimental mimicry demonstrate that this approach can expand the key space and fend off frequent attacks. The work in [17] introduced a new, safe image encryption technique that makes use of a substitution box (S-Box) and chaos-based random number generator. Substitution-box, one of the main crucial block cipher elements is utilized in the new encryption technique. System analyses showed that it contains dynamic properties that are sufficiently complex. An encrypting images procedure using a random sequence of iterations work on various replacement techniques is provided in [18].

The main concept is based on the fact that by employing specific permutation techniques, by minimizing the association between the bits, pixels, and blocks, it is possible to reduce the amount of information that can be perceived in a given image. The findings show that the combined strategy overcomes the drawbacks of these methods, such as visual intelligence and redundancy, and achieves the benefits of the distinct permutation approaches. The concept of a genetic algorithm-based encryption solution for monochrome medical images is presented in [19]. The algorithm's robustness is increased by repeating the crossover and mutation stages, each of which depends on a different key. Performance evaluations reveal that the suggested scheme has high statistical properties, key sensitivity, and effective resistance to brute-force, differential, plaintext, and entropy attacks.

3. Advanced Encryption Standard

The National Institute of Standards and Technology (NIST) initiated the DES replacement selection process in 1997. Based on competitive selections, the submission that was made the standard was the advanced encryption standard cipher. This symmetric block cipher known as the AES is selected by the United States government to secure sensitive data. To encrypt confidential data as depicted in Figure 1, AES is used in hardware and software worldwide with different block lengths and ciphertext spaces. For public computer security, cybersecurity, and the protection of technological data, it is essential. The substitution and permutation concepts are the foundation of the AES algorithm's security for each stage and provide confusion as well as diffusion across all cipher stages.

The structure of AES employs an adjustable key size of 128, 192, or 256-bits with regard to 10, 12, or 14-rounds of the number of rounds Nr, respectively, and a 128-bits input text

block. The encryption step is one of many processing stages that are included in each round and transformation to provide the final ciphertext. Similar to this, encryption text is transformed back into plaintext using a sequence of reverse rounds [20]. The rounds are played in the order stated, with the exception of the first and last rounds. The last round does not have a column transformation step, and the first round has an additional step of the round key stage. Moreover, AES is set up with a mode that modifies the encryption of data blocks. Cipher-block chaining configurations include one of these modes [21].

The initialization vector is first applied solely to the initial block of plaintext, and after that, the input of the following block and the ciphertext of the previous block are bitwise XORed. Till the final block of the plaintext is reached, with bitwise XOR procedure is iterated and repeated.

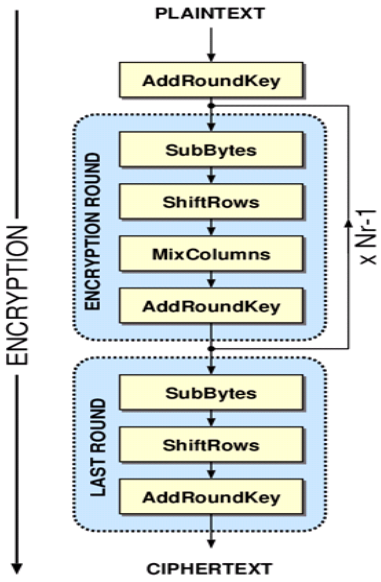

Figure 1. Basic structure of encryption AES encryption model.

4. The Proposed Medical Image Encryption

4.1. Expansion of the Key

The function of the AES key extension algorithm requires an input of 4-word key bits which represents a 16-byte and on the other hand, produces a linear array of 44-words that act as the expanded key of 176 bytes. Such an operation is considered appropriate to supply a 4-word running key for the first AddRoundKey step and each of the key expansion transformations across the residual rounds of the AES ciphering algorithm thereafter.

The following pseudocode characterized the key expanded entire process:

For (z = 0 ; z < 4 ; z++)

[K[4*z] , K[4*z+1] , K[4*z+2] , K[4*z+3]]

EndFor

For (z = 4; z < 44 ; z++)

foo = w[z – 1]

If (z mod 4 = 0) Then

foo = SubWord (RotWord (foo)) XOR Rcon[z / 4]

w[z] = w[z – 4] XOR foo

EndIf

EndFor

The first for-loop repeated to supply the 4-word key bits while the second loop executes a one-byte circular left shift (CLS) over the result words using the RotWord process and conducts a byte replacement on every byte of the word it receives using the AES S-box SubWord transformation. Rcon value is considered as a round constant which is XORed with the first part resulting from the byte substitution procedure.

4.2. NIST Test of Randomness

A statistical analysis with up to 15 tests called the NIST test suite is represented in Table 1, [22]. The fifteen tests are designed to assess the randomness of the key bit-strings generated by the key extension function. Expansion of the used key is considered for each round of the AES transformation. The high p-values of key-based bit-string indicate that the suggested algorithm generates extremely random key bits.

Table1. Test results for key extension function results.

Test	P-value	Result
Block frequency	0.92548	Pass
Frequency	0.21592	Pass
Cusum (F)	0.38446	Pass
Cusum (R)	0.24784	Pass
Long runs of ones	0.13597	Pass
Spectral DFT	0.42201	Pass
Rank	0.84258	Pass
Lempel Ziv complexity	1.00000	Pass
Overlapping templates	0.17084	Pass
NonOverlapping templates	0.60892	Pass
Approximate entropy	0.71449	Pass
Universal	0.51071	Pass
Random excursions	0.57632	Pass
Serial (m = 16)	0.46705	Pass
Random excursions variant	0.83109	Pass
Runs	0.71225	Pass
Linear complexity	0.73846	Pass

4.3. Image Encryption

This work studied the privacy enhancement of medical images based on AES. The input image is divided into subblocks based on the 128-bit constraint. The results of the image encryption-based AES algorithm are done successfully.

The method of encrypting an image converts it to bits and then divides it into blocks of 128-bits where each block consisting of 16-bytes then, the AES encryption procedure is applied as depicted in Figure 2. The image subblocks are encrypted with a 128-bit key. The associated AES is known as AES-128, or AES-256 relying on the size of the secret key, which can be 128 or 256-bits. The additional rounds and slower encryption performance are associated with AES's longer secret key. The slowest AES is therefore AES-256, which is followed by AES-192 and AES-128. It is important to note that there isn't an official report on the AES security problem. The AES structure consists of one key expansion and a number *Nr* of rounds functions. The values for Nr are 10 and 14 for AES-128 and AES-256 respectively. The following steps outline the essential features of this process.

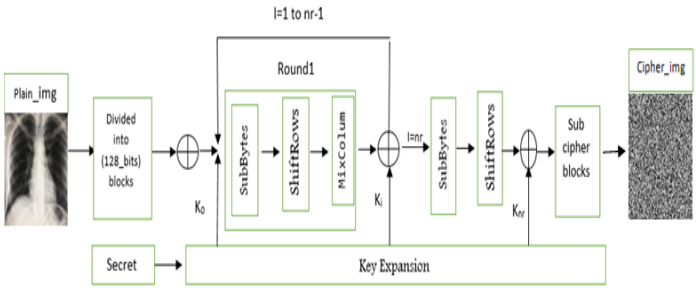

Figure 2. Medical image encryption with AES enhancing model.

The process of AES-128 requires Nr=10 rounds of encryption while the number of words that are input keys is represented by Nk=4, and the key value is ”abcdefghijklmnop”. The following algorithm describes the medical image encryption entire process:

Step **1**: Divide the image file into bits that each block composed of 128-bits and then into 16 groups and store them in an array of bytes.

Step **2**: Key expansion function that extended 128-bits key to a word *w* consists of w[4*(Nr+1)] bytes.

Step **3**: Procedure image_encryption.

- For each 128-bits image block do:

AddRoundKey: round key plus transform - XOR for each column with the extended key.

- For round = 1 to round = Nr-1

1. SubBytes: that making S-Box conversion - the last 4-bits are column numbers while the first 4-bits are line numbers.
2. ShiftRows: Line transform - byte cyclic shift.
3. MixColumns: Column transformation.
4. AddRoundKey transformation.

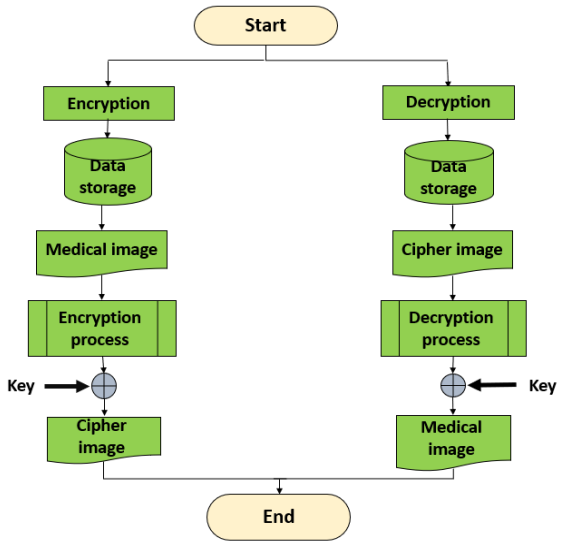

Figure 3. Flowchart of the encryption/decryption processes.

Step **4**: Final round that round =Nr

- SubBytes.
- ShiftRow.
- AddRoundKey.
- Encryption blocks_img.

Step **5**: Output encryption image.

4.4. Image Decryption

It is a reverse process of medical image encryption as depicted in Figure 3. In this process, the encrypted image is considered as input for the AES algorithm structure for decryption. The encrypted image is divided again into 128-bits subblocks that are the same as the AES algorithm block length. After completion of decryption, the obtained output is considered as the decrypted image, it follows the same characteristics as the original image.

5. Results and Security Analysis

Medical image encryption and decryption are implemented in this paper, using C++ programming software and open CV. Here we adopt the standard test images chest and brain images as the experimental samples with size 128x128 to encrypted and decrypted using AES methodology.

5.1. Key-Space Structure

A fundamental characteristic of image-encrypted schemes should be the sensitivity of the produced keys and the initial parameters that are employed in encryption. It is known that the mitigation of brute-force attacks is due to the use of powerfully built key space. Different key sizes that can take part in the encryption process are included in that large-scale space. According to [23], key size wide-ranging is customarily forecasted to be over a range of 2100. In the AES method with a key length of 128-bits, the corresponding key space is equal to 2128. In our experiments, the total key space is more than 2100, which means that it is adequate to stand up to exhaustive attacks.

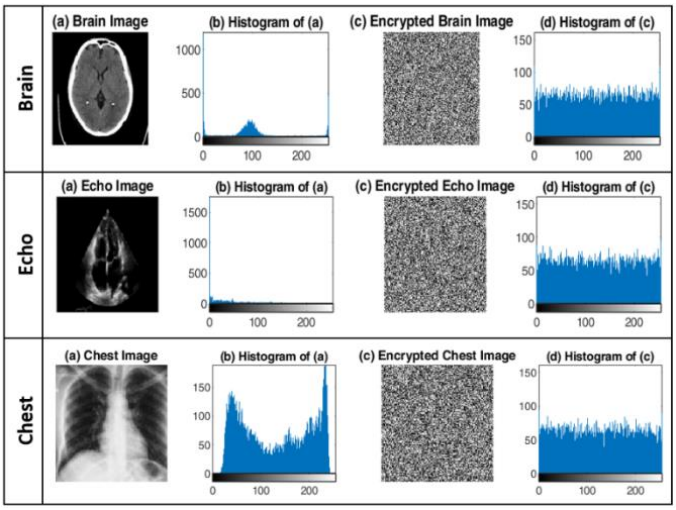

Figure 4. Histograms of three medical plainimages and the corresponding cipherimages.

5.2. Histogram Analysis

To avoid information leakage to the opponent, the guarantee that the output encryption image has no statistical likeness to the corresponding plainimage is mandatory [24]. In Figure 4, the histograms of three medical plainimages are plotted and compared with the corresponding ciphered images. It is shown that the histograms of the plainimages have large spikes. Also, the histograms of the corresponding cipherimages are nearly smooth and symmetric, which indicates that each of the image pixels is evenly potential to occur. The extrovert cipherimages vary significantly from the plainimage's histograms. As a result, they possess an indication that the suggested encryption method is susceptible to any statistical attack.

5.3. Entropy Analysis

Information entropy is a term used to describe how random the content of an image is. Equation (1) is an illustration of how the entropy H(m) of message m can be identified.

$$H(m) = \sum_{i=0}^{N-1} P(m_i) \log_2 \frac{1}{P(m_i)} \qquad (1)$$

Where $P(m_i)$ refers to the probability of symbol m_i occurrence and $\log_2$ denotes the base of 2 logarithmic functions [24]. Three source test images and matching encrypted images are provided with resulting entropy values in Table 2.

These entropy levels are quite near to the theoretical value of 8. This denotes that all image pixels that are encrypted have an equal chance of occurring. As a result, the cipherimages' data leakage is minimal, and they are protected from entropy-based attacks.

5.4. Correlation Analysis

Any two adjacent pixels in a given image have higher vertical, horizontal, and diagonal correlations with one another. The maximum and minimum values of the correlation coefficient are one and zero, respectively [24]. For the three test plainimages and the corresponding cipherimages, the correlation coefficient (CC) values are obtained and are recorded in Tables 3 and 4 in the appropriate order.

Table 2. Entropy values of three medical images and the resulting cipherimages

Test image	Original	Cipherimage
Brain	4.6419	7.9862
Echo	3.1398	7.9873
Chest	7.6616	7.9884

Table 3. Correlation analysis of three test medical images

Plainimage	Correlation coefficient		
	vertical	horizontal	diagonal
Brain	0.948845	0.921519	0.890406
Echo	0.939146	0.933356	0.880098
Chest	0.991599	0.988318	0.981372

The values obtained show that, although these pixels are significantly associated within the plainimages, a weak association between them is found in the cipherimages.

Table 4. Correlation analysis of the encrypted images

Cipherimage	Correlation coefficient		
	vertical	horizontal	diagonal
Brain	-0.001540	-0.004175	-0.005528
Echo	0.006992	-0.023371	-0.000050
Chest	0.000069	-0.000032	0.000987

5.5. Diffusion Analysis

It is presented in [25] that the measure of a number of pixels change rate (NPCR) with the unified average change intensity (UACI) test is used to quantify diffusion and ambiguity requirements for image encryption. The estimated NPCR and UACI rates for a 256 gray-level image are 99.61% and 33.46%, respectively [26]. A key component of an image cryptosystem's effectiveness and security might be considered to be its diffusion performance.

Table 5. Results of NPCR and UACI tests for the encrypted images

Cipherimage	NPCR%	UACI%
Brain	99.52	40.96
Echo	99.49	45.63
Chest	99.62	33.28

For each of the plainimages, the NPCR and UACI experimental results are shown in Table 5. The UACI is found to be above 33%, and the NPCR is over 99%. According to the findings, even slight modifications to the original image can significantly influence the cipher-image, making the suggested scheme resistant to differential attacks.

6. Conclusion

An enhanced medical image privacy model has been developed in this work to create a robust symmetric image privacy method. To address the issue of textured zones seen in other well-known encryption methods, the AES is expanded with the goal of utilizing key stream generators to encrypt medical images. The proposed system offers good security and is easily implementable in terms of protection against statistical analysis attacks, according to the test results analysis. The performance of encryption is significantly impacted by the key expansion process. Future research will be done on the application of the suggested strategy in a cloud storage system. More evaluation will be done on the suggested method's crypto stability as well as how to speed up its performance across various platforms.

CRediT authorship contribution statement:

O.Reyad, conceptualization, idea proposal, editing, and preparation; H.Mansour, data curation, software, writing, and preparation; E.Zanaty, editing, review, and supervision; M.Heshmat, preparation, visualization, and review. All authors have read and agreed to this version of the manuscript.

Data availability statement

The data used to support the findings of this study are available from the corresponding author upon request.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

[1] S. H. Kamali, R. Shakerian, M. Hedayati and M. Rahmani, *International Conference on Electronics and Information Engineering*, Kyoto, Japan, (2010) 141-145.

[2] M. K. Hasan et al., *in IEEE Access*, 9 (2021) 47731-47742.

[3] O. Reyad, M.E. Karar, *Arab J. Sci. Eng*, 46 (2021) 3581–3593.

[4] C.A. Weaver, M.J. Ball, G.R. Kim, J.M. Kiel, *Health Informatics, Fourth edition, Springer Cham*, (2015).

[5] K. Shankar, M. Elhoseny, E. Perumal, M. Ilayaraja, and K. Sathesh Kumar, in *Proc. Adv. Sci. Technol. Secur. Appl*., (2019) 31-42.

[6] A. Ahmad, Y. AbuHour, R. Younisse, Y. Alslman, E. Alnagi, Q. Abu Al-Haija, *Journal of Sensor and Actuator Networks* 11 (2022).

[7] M.E. Karar, F.Z. Khan, H. Alshahrani, O. Reyad, *Alexandria Engineering Journal*, 69 (2023) 571-583.

[8] W.M. Abd-Elhafiez, O. Reyad, M.A. Mofaddel, M. Fathy, *In: Hassanien, A. et al. (eds.) AMLTA* (2019), *AISC* 921, *Springer, Cham* (2020) 645–655.

[9] T.K. Araghi and A. A. Manaf, *Future Gener. Comput. Syst.*, 101 (2019) 1223-1246.

[10] S. J. Shackelford, M. Mattioli, S. Myers, A. Brady, Y.Wang, and S.Wong, *Minn. JL Sci. Tech.*, 19 (2018) 405.

[11] W. Stallings, L. Brown, *2nd Ed. Pearson*, (2012).

[12] A. Hafsa, A. Sghaier, J. Malek, and M. Machhout, *Multimed. Tools Appl*., 80 (2021) 19769–19801.

[13] R.S. Bhogal, B. Li, A. Gale, and Y. Chen, *Int. J. Inf. Technol. Comput. Sci*., 10 (2018) 1–10.

[14] M. Zeghid, M. Machhout, L. Khriji, A. Baganne, and R. Turki, *Int. J. Comput. Sci. Eng.*, 1 (2007) 745-750.

[15] O. Reyad, K. Hamed, M.E. Karar, *J. Intell. Fuzzy Syst*, 39(5) (2020) 7795–7806.

[16] Y. Wan, S. Gu, and B. Du, *Entropy*, 22 (2020) 171.

[17] Ü. Çavuşoğlu, S. Kaçar, I. Pehlivan, A. Zengin, *Chaos, Solitons & Fractals*, 95 (2017) 92-101.

[18] A. Mitra, Y. V. S. Rao, and S. R. M. Prasanna, *Int. J. Electr. Comput. Eng.*, 1 (2006) 127-131.

[19] N. K. Pareek and V. Patidar, *Soft Comput.*, 20 (2016) 763-772.

[20] M. Dworkin, E. Barker, J. Nechvatal, J. Foti, L. Bassham, E., Roback, J. Dray, *Federal Inf. Process. Stds. (NIST FIPS), Gaithersburg, MD*, (2001).

[21] B. Schneier, *New York, NY, USA* (1995).

[22] A. Rukhin, J. Soto, J. Nechvatal, et al., *NIST Special Publication* (2001) 800–22.

[23] X.Wang, L. Teng and X. Qin, *Signal Process* 924 (2012) 1101–1108.

[24] R.C. Gonzalez and R.E. Woods, *Prentice-Hall, Inc., Upper Saddle River, NJ*, (2006).

[25] G. Zhang and Q. Liu, *J Optics Communications* 284 (2011) 2775–2780.

[26] Y. Wu, J.P. Noonan, and S. Agaian, *IEEE Transl J of Selected Areas in Telecommunications (JSAT)*, (2011) 31–38.