ISSN 2303-4521
Original Research
Periodicals of Engineering and Natural Sciences
Vol. 9, No. 4, November 2021, pp.928-947

Enhancement to the patient's health care image encryption system, using several layers of DNA computing and AES (MLAESDNA)

Jamal Kh-Madhloom[1,2] *, Mohd Khanapi Abd Ghani[1] and Mohd Rizuan Baharon[1]
[1] BIOCORE Research Group, Faculty of Information & Communication Technology, Universiti Teknikal Malaysia Melaka, Melaka, 76100, Malaysia
[2] Computer Science Department, College of Computer Science and information technology, University of Wasit, Wasit, 123, Iraq

ABSTRACT

Keeping patient health data private has been a big issue for decades, and this issue will not go away anytime soon. As an integral part of many developing technologies, cryptographic Internet communications ICs (e.g. fog computing and cloud computing) are a main focus of IoT research. Just keep trying all the potential keys until you find the correct one. New and future technologies must have a model of DNA cryptography in order to assure the efficient flow of these technologies. Public-key cryptography is also required to make DNA sequence testing devices for the Internet of Things interoperable. This method employs DNA layers and AES in such a way that it may be easier to design a trustworthy hybrid encryption algorithm that uses DNA layers and AES. In order to guard against brute-force decryption attacks, DNA sequences are encrypted using three keys: (I) the main key, which is the key to the AES encryption algorithm; (II) the rule 1 key, which is the base DNA structure; and (III) the rule 2 key, which is the DNA helical structure binding probability. This key was created with increased security in mind. multi-layered AES encryption and DNA computing were applied to "Covid 19" images in this research (MLAESDNA). With cloud computing, the MLAESDNA team was able to show that IoT signals could be enhanced with encrypted data.

Keywords: Covid 19 images encryption, DNA computing; MLAESDNA; IOT; AES

Corresponding Author:

Jamal Kh. Madhloom
BIOCORE Research Group, Faculty of Information & Communication Technology
Universiti Teknikal Malaysia Melaka
Melaka, 76100, Malaysia
E-mail: jamalkh@uowasit.edu.iq

1. Introduction

Cryptography is the study of keeping secret information safe. The second area, cryptanalysis, deals with vulnerabilities in cryptographic schemes. Cryptography relies on mathematics as its foundation, and cryptanalysis employs it. Encryption, the act of converting data and information into a useless format for anybody who is not granted access, is often described as "cryptography." Decryption was originally used to protect military and diplomatic communications from being exposed. Cryptography is defined as the study of message encryption and decryption, with the primary aim of keeping information private. Cryptography has grown more prevalent, not just among companies, but also among people, with the proliferation of the information economy and the transfer of sensitive information through untrusted mediums. Over the last few decades, the breadth of data transmission has expanded beyond the realm of information exchange and entertainment to include almost all aspects of ISM activity [1].

"Cryptography" in current implementations might entail a lot more than just encrypting and decrypting for the user. Other areas of information security are also safeguarded by encryption techniques. In addition to message authentication, sender and recipient identification, message integrity, and the non-repudiation of the message transmission, they include message authentication, sender and recipient identity, message integrity, and the non-repudiation of the message transmission. In contemporary use, "cryptography" can refer to a variety of techniques and applications for storing and transmitting information, as well as methods used to ensure the security of stored data. With regard to IoT, cloud computing and fog computing have made data accessible to software programs and their users, resulting in greater data collection and sharing. [4] believes that the internet of things consists of gadgets that are physically connected to the internet, where information is gathered and shared. It is easier now to link computer systems to the physical world thanks to the concept of the Internet of Things. Several sectors are predicted to profit greatly from the Internet of Things, including telemedicine systems and health care. Patients who participate in the program should expect better health-care services. Since the creation of IoT healthcare apps during the last several years, healthcare professionals have been striving to create more dependable and secure Internet of Things healthcare applications to increase healthcare services and to help patients with chronic conditions who are away from home. Similarly, to Covid 19, these apps are gathering patient data and providing treatment through a wide variety of sensory devices.

Electronic medical records, film X-rays, paper EKGs, and other types of hard copy are being phased out in favour of digital data. Paper records, film X-rays, paper EKGs, and other types of hard copy are being archived for seven years on inactive patients who may never be seen again. X-rays, MRIs, CT scans, EKGs, and patient data, among other things, are either generated digitally or digitized to make retrieval easier and, in certain cases, to reduce the amount of physical storage space required. Patients may also enter data, do medical research, and even check in for appointments via kiosks that are connected to the Internet of Things, which will ultimately eliminate the mountains of paper that were generated by previous record systems. The large number of Internet of Things devices involved make the shift to digital medicine easier. X-ray equipment have progressed to become Internet of Things (IoT) devices. Instead of using film to record the images, sensors implanted in the X-ray plate detect the X-rays and convert them into a digital representation. This image is then sent over the internet, where it may be seen by technicians and other medical experts. Frequently, the photographs are reviewed before they are shown to the doctor. Artificial intelligence (AI) is increasingly being used to detect problems more rapidly than a human specialist can do on a given subject. In a typical Internet of Things (IoT) system, sensor devices, cloud-based interfaces, machine algorithms, and sensors embedded in the X-ray plate are all included. Sensor devices, such as Covid 19 X-Rays pictures, are used to collect information about the human body from the environment. In contrast, sensors embedded inside the X-ray plate allow for communication [7]. To perform the necessary analysis, algorithms must first evaluate the data that has been collected [8]. Users [9], whether they are patients or healthcare professionals, may also access data stored in cloud services since they are accessible via a web browser. [10] It has been secured and protected in order to improve patient well-being, IoT healthcare applications must take into consideration the security and privacy issues that they raise in patients' lives, in addition to additional repercussions such as data breaches and financial risks. This article examines the components of the application architecture in order to handle privacy and security issues in Internet of Things healthcare applications.

Fog computing was designed to connect Internet of Things devices to data center servers. Fog computing is primarily focused on reducing the time it takes to compute. Fog computing is often an excellent choice for certain IoT applications due to cloud computing's inaccessibility. Due to the numerous benefits, which include decreased latency, cheaper bandwidth utilization, and improved security, fog computing is an excellent solution for IoT applications. In contrast to fog, which causes safety and privacy difficulties, the properties of fog raise substantial security and privacy issues [6]. While cloud computing security and privacy safeguards can't be applied directly on fog [8, as they can in other computing environments], current cloud computing security and privacy protections aren't a viable option for use in fog [8]. There are numerous security risks with using fog computing for Internet of Things systems, including CIA, confidentiality, integrity, and availability. In order to explore these security concerns, we explored the consequences of deploying a smart metering system using fog computing. Regarding security and privacy, fog's properties cause considerable concerns. New security and privacy safeguards for cloud computing are not applicable to fog computing (which can also be referred to as “stealth computing”). Fog computing for IoT systems presents significant security risks, which we researched when assessing a Fog Computing Gateway (FCG) protection failure [8].

To achieve this goal, this article proposes the development of a multilayer trustworthy system for DNA sequences, which would combine DNA computing and the AES algorithm. By using DNA computers to apply and integrate this method into a biological context, this technique will be capable of protecting the DNA sequence from plain-text assaults via the creation of main key and rule key sequences. The article makes a number of important contributions, including the ones listed below: I It includes: I A multilayer encryption algorithm that incorporates DNA and the AES algorithm; ii) A secure encryption technique for IoT-based medical healthcare systems; iii) An encryption technique that reduces the length of Covid 19 X-Ray images and thus reduces the complexity of complex mathematical operations; and iv) An encryption technique that increases the amount of encryption power.

The rest of this article is arranged in the following manner: Section 2 provides an overview of current related work. Section 3 goes into great depth on the process for the suggested model. Section 4 includes the results of the experiment as well as a commentary of the results. Finally, in Section 5, we end our investigation.

2. Related work

The challenge for healthcare organizations is keeping up with the rapid rise of telemedicine and healthcare applications. This is a critical issue as both health records and medical data must be transmitted securely over the internet or via any other means. As the graphic shows, this compulsion led academics to direct their attention to improving and/or inventing new encryption algorithms that would better suit this objective.

Table 1. AES Enhancements Advantages

Ref	Existing Methods	Advantages
[11]	• Modified-AES images-ciphering especially the HD.	• great security.
[12]	Data Encryption Standard, Triple DES &Advanced Encryption Standard.	Dynamic “key-generation”, “Key-values manipulation” & Improved security.
[13]	==	Hiding data “DNA sequence” & “deep learning”.
[14]	RSA, DES &NTRU.	Build “DNA-basis” system, Suits biological environment .
[15]	==	Applicable to any kind of data.
[16]	==	Analysis of security is tested by NIST Test Suite.
[17]	DES, IDEA & AES.	Adjustment of ShiftRow, no additional operations or hardware needed.
[18]	ECC and GEO	IoT data confidentiality.

Over the course of many years, researchers have released a number of encryption enhancement experiments in the steganography sector, which have been compared and analyzed in this study. To combat the tremendous computational power of today's computers, especially the future generation of quantum computing devices, there is a broad trend toward strengthening a new encryption method. The mathematical and theoretical underpinnings of cryptographic systems have always been strong throughout the history of the field. As a consequence, as shown in Table 1, a number of researchers were interested in developing a new AES encryption technique that was based on DNA. This is beneficial for all technologies that deal with a high number of linked devices and sensitive data storage, as well as data exchange between these devices on a consistent basis. So security and privacy are important concerns in this and other applications. Furthermore, systems must be capable of fulfilling data security requirements across the board. Throughout the study, we looked at a number of different AES enhancement studies that were conducted utilizing a range of different techniques. In addition, we examined 11 peer-reviewed publications to establish the degree to which encryption techniques for data transmission have been improved in different applications during the last several years. Recent research articles on AES have concentrated on the use of DNA to increase the encryption's strength, and have proposed algorithms to address issues such as high capacity, unpredictable and high deterioration steganography techniques, which ensure that even if the system is compromised, the data is not visible to hackers In this paper, we have focused our study on the AES algorithm and DNA, both of which have been the topic of earlier studies by other researchers. We looked at a number of different methods and found that the current trend is to utilize DNA to improve the performance of the AES algorithm. Additional study and evaluation of conventional encryption methods, along with their related difficulties, was conducted.

Our analysis demonstrates that key research areas, such as the use of AES and DNA hybrid systems, are underrepresented.

AES is an encryption algorithm that is extensively used and was developed by the National Institute of Standards and Technology (NIST) to replace the DES algorithm [19]. For data packets to be encrypted and decoded, the AES algorithm first encrypts them for a total of 10 rounds using 128-bit encryption keys, then for a total of 12 iterations using 192-bit encryption keys, and finally for a total of 14 iterations using 256-bit encryption keys to generate the final encrypted message. The flowchart for the AES is shown in Fig. 1 [20-24].

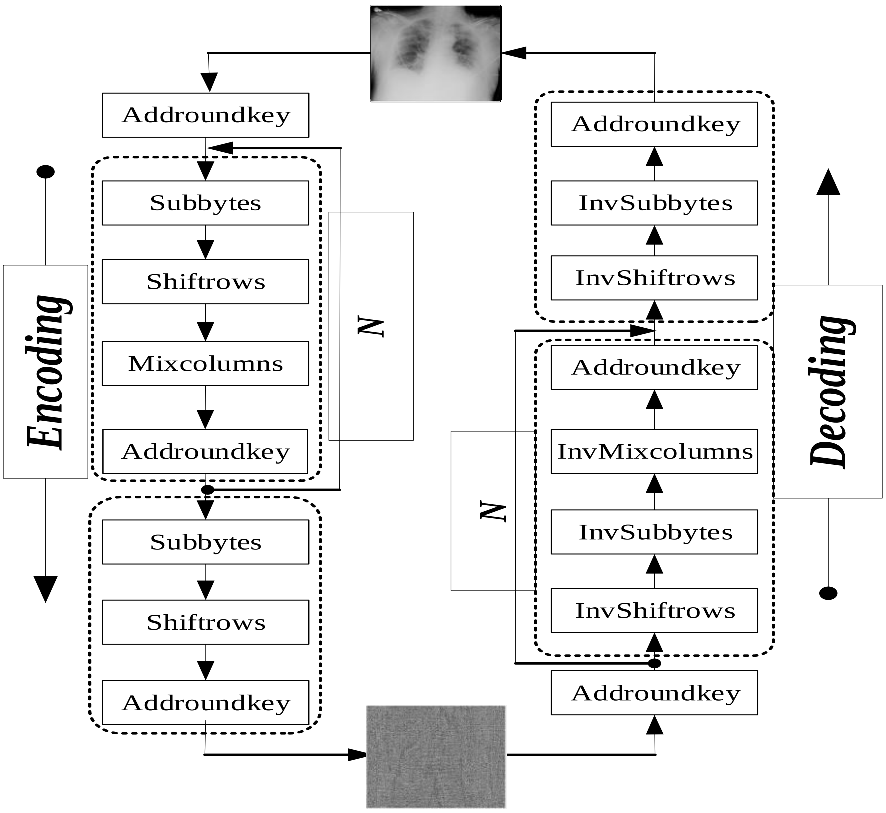


Figure 1. Flowchart of AES Encryption [25]

The proposed technique utilizes photographs of 256 x 256 pixels and a simplified AES block encryption (which is round in shape) to perform DNA computation. a technique for encrypting high-definition photographs that has been implemented in software was disclosed by [25]. In the beginning, when the AES block cipher algorithm was created, it had the drawback of processing time being increased and the number of rounds being reduced owing to encryption attacks. To accomplish the same goal, a hybrid RSA/AES encryption technique has been proposed for cloud computing [27]. With RSA and AES encryption, three keys are created: a public key for encryption, a private key for encryption, and a secret key for decryption. Encryption's public key, its private key, and its secret key. Current study claims that including a Polybius matrix in the AES data security algorithm yields higher safety because it raises the number of rounds available in the method (Singh, 2013). Additionally, the challenge was to use chaotic maps to generate a key to use in encrypting with the AES technique. Also, [27] describes a digital image encryption approach, which used the AES encryption algorithm to accomplish encryption and decryption functions, and showed its usefulness by carrying out those operations.

A fundamental discovery is that it is possible to use and research biological molecules in order to conduct complex mathematical computations, an area that is relatively young. Compassionate [compassionate] The idea of employing biological neurons and molecules to carry out calculations in place of using computers is called a DNA calculation. Simply put, a DNA computer is a conglomeration of DNA strands that have been utilized to deal with a computational problem. Technological advances have allowed for the selective assortment of strands and the management of solutions, resulting in the resolution of larger and more complex computing issues far more quickly than conventional computers [28-32].

3. Methodology

The cryptographic algorithms that are now in use are mathematical in nature. DNA-inspired algorithms are a combination of both current and emerging cryptography technologies that are based on genetic information. This section describes the MLAESDNA data encryption technique, which is a hybrid of the AES and DNA computing technologies. The MLAESDNA project's purpose is to increase security by increasing the key length by leveraging the DNA layers surrounding the AES algorithm; this will result in the prevention of unauthorized users' pirating content.

MLAESDNA uses DNA computing technologies to supplement the AES encryption layer, which is currently in use. The numerous modifications of the encryption process are carried out in a step-by-step manner to the final state [22]. Binarization of X-ray images and DNA conversion are among the transformation layers. It demonstrates the encryption and decryption processes using the multi-layer DNA and AES algorithms proposed in the suggested paradigm. MLAESDNA aspires to improve the AES algorithm in order to obtain the highest level of security possible for data transmission. In the DNA and AES algorithms, the amount of security is determined by the length of the key used. When the AES algorithm is used, it repeats the identical procedures over and over again for a predetermined number of rounds. The round count of the algorithm is proportional to the size of the key. The proposed approach makes use of a 128-bit block cipher and N rounds of encryption.

By using DNA Encryption to extend the key length, the AES becomes more complicated and therefore more resistant to technological progress. The suggested algorithm's key length is (24 *2128 * 3 * 10) bits, which is computed as follows:

a) **Key 1:** DNA key size is 24. The probability of the key: A= 11 or 10 or 01 or 00, T= 11 or 10 or 01 or 00, C= 11 or 10 or 01 or 00 and G= 11 or 10 or 01 or 00.
b) **Key 2:** AES key size is 2128.
c) **Key 3:** key size = 3 according to three different DNA bases (A=C, G=T) or (A=G, T=C) or (A=T, G=C).
d) **Key 4:** AES round = 10.

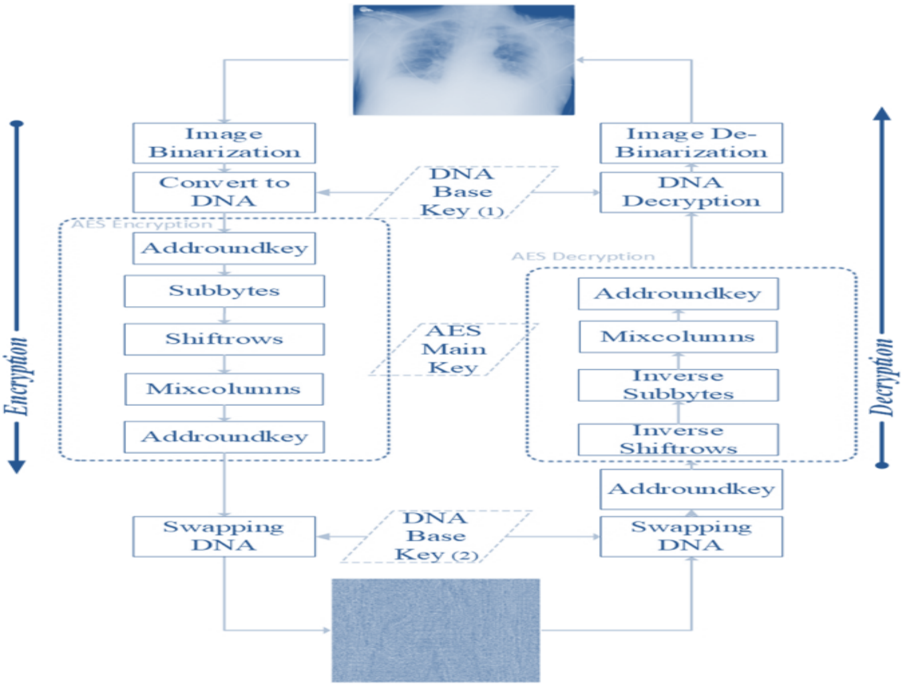


Figure 2. Flowchart of the MLAESDNA

3.1. Steps of proposed method

This section provides an overview of the stages that are performed during the algorithm's operation; each subsequent step is critical to the algorithm's operation and was developed with algorithm design considerations in mind to generate superior algorithm performance metrics.

a) Image Binarization “Pre-Processing”

As shown in Fig.3, this phase entails transforming the Covid 19 picture to binary bits using MATLAB algorithms that are optimized for DNA conversion.

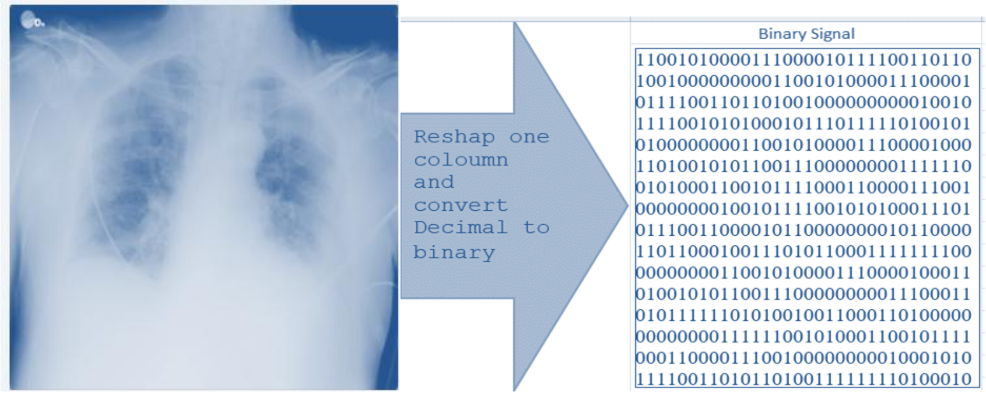


Figure 3. Flowchart of the greyscale image pre-processing

b) Converting to DNA

The DNA Encryption method begins by converting the binary message acquired in the previous step into a DNA helix using varied DNA bases. DNA Rule (1) "key size is 16" is shown in Table 2. Figure 4 illustrates a DNA helix conversion sample.

Table 2: DNA rule (1) with key size=16.

Rules	A	T	C	G
Rule 1.1	11	10	01	00
Rule 1.2	11	10	00	01
Rule 1.3	11	00	10	01
Rule 1.4	00	11	10	01
Rule 1.5	00	11	01	10
Rule 1.6	00	01	11	10
Rule 1.7	01	00	11	10
Rule 1.8	01	00	10	11
Rule 1.9	01	10	00	11
Rule 1.10	10	01	00	11
Rule 1.11	10	01	11	00
Rule 1.12	10	11	01	00
Rule 1.13	10	11	00	01
Rule 1.14	10	00	11	01
Rule 1.15	00	10	11	01
Rule 1.16	00	10	01	11

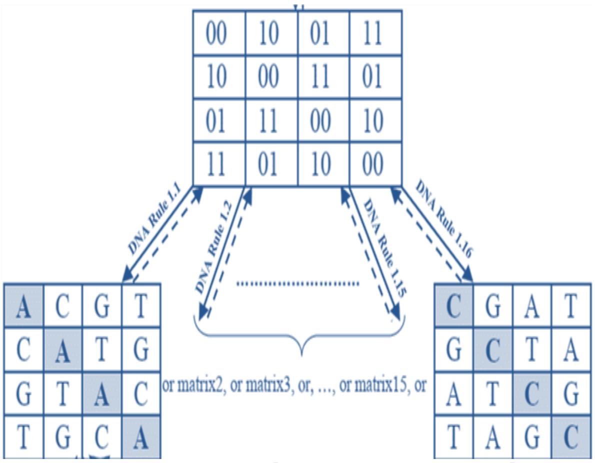


Figure 4. DNA-Helix conversion sample

c) SubBytes

The SubBytes operation is a non-linear byte replacement that operates separately on each byte of the state, as shown in Figure 5. SubBytes is the inverse of SubBytes; it uses the inversed S-Box, which is likewise pre-calculated as illustrated in Fig.6. Each byte in the state is replaced with its entry in a fixed 8-bit lookup table, S, in the SubBytes step; b (I, j) = S. (i, j). Tabular representations of the S-Box and Inverse S-Box tables are shown in Tab. 3 and 4. The SubBytes and InvSubBytes transformations are mutually exclusive.

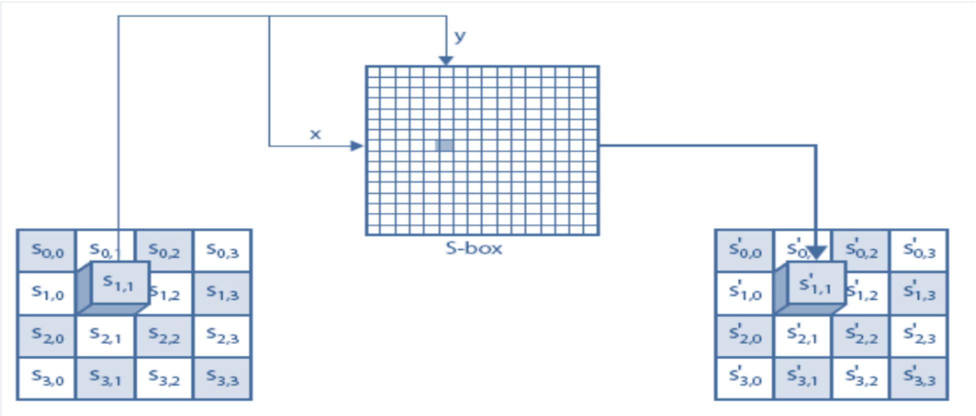
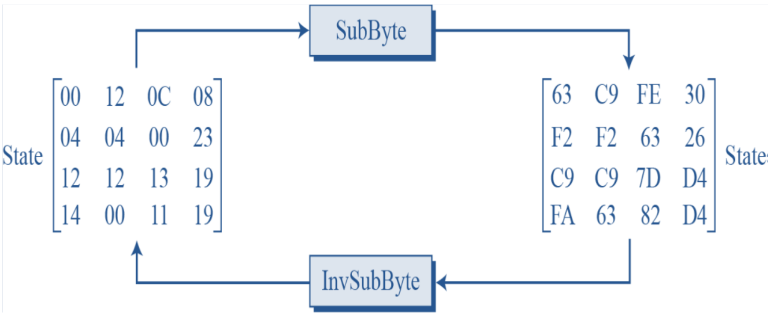

y
x
S-box
$s_{0,0}$ $s_{0,1}$ $s_{0,2}$ $s_{0,3}$
$s_{1,0}$ $s_{1,1}$ $s_{1,2}$ $s_{1,3}$
$s_{2,0}$ $s_{2,1}$ $s_{2,2}$ $s_{2,3}$
$s_{3,0}$ $s_{3,1}$ $s_{3,2}$ $s_{3,3}$
$s'_{0,0}$ $s'_{0,1}$ $s'_{0,2}$ $s'_{0,3}$
$s'_{1,0}$ $s'_{1,1}$ $s'_{1,2}$ $s'_{1,3}$
$s'_{2,0}$ $s'_{2,1}$ $s'_{2,2}$ $s'_{2,3}$
$s'_{3,0}$ $s'_{3,1}$ $s'_{3,2}$ $s'_{3,3}$

Figure 5. SubBytes Representation



$$\begin{bmatrix} 00 & 12 & 0C & 08 \\ 04 & 04 & 00 & 23 \\ 12 & 12 & 13 & 19 \\ 14 & 00 & 11 & 19 \end{bmatrix} \quad \begin{bmatrix} 63 & C9 & FE & 30 \\ F2 & F2 & 63 & 26 \\ C9 & C9 & 7D & D4 \\ FA & 63 & 82 & D4 \end{bmatrix}$$

Figure 6. SubBytes and Inverse of SubBytes Transformations

Table 2. S-Box Table

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
A	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
B	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
E	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
F	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

Table 3. Inverse S-Box Table

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	52	09	6A	D5	30	36	A5	38	BF	40	A3	9E	81	F3	D7	FB
1	7C	E3	39	82	9B	2F	FF	87	34	8E	43	44	C4	DE	E9	CB
2	54	7B	94	32	A6	C2	23	3D	EE	4C	95	0B	42	FA	C3	4E
3	08	2E	A1	66	28	D9	24	B2	76	5B	A2	49	6D	8B	D1	25
4	72	F8	F6	64	86	68	98	16	D4	A4	5C	CC	5D	65	B6	92
5	6C	70	48	50	FD	ED	B9	DA	5E	15	46	57	A7	8D	9D	84
6	90	D8	AB	00	8C	BC	D3	0A	F7	E4	58	05	B8	B3	45	06
7	D0	2C	1E	8F	CA	3F	0F	02	C1	AF	BD	03	01	13	8A	6B
8	3A	91	11	41	4F	67	DC	EA	97	F2	CF	CE	F0	B4	E6	73
9	96	AC	74	22	E7	AD	35	85	E2	F9	37	E8	1C	75	DF	6E
A	47	F1	1A	71	1D	29	C5	89	6F	B7	62	0E	AA	18	BE	1B
B	FC	56	3E	4B	C6	D2	79	20	9A	DB	C0	FE	78	CD	5A	F4
C	1F	DD	A8	33	88	07	C7	31	B1	12	10	59	27	80	EC	5F
D	60	51	7F	A9	19	B5	4A	0D	2D	E5	7A	9F	93	C9	9C	EF
E	A0	E0	3B	4D	AE	2A	F5	B0	C8	EB	BB	3C	83	53	99	61
F	17	2B	04	7E	BA	77	D6	26	E1	69	14	63	55	21	0C	7D

d) ShiftRow Operation

ShiftRows is the inverse of ShiftRows. It does the same cyclic shift, but to the right. It is required for decoding later. The ShiftRows step cyclically shifts bytes in each row of the state to the left. Each row has a unique number of locations where each byte is shifted. ShiftRows schema and example are shown in Figures 7 and 8, respectively.

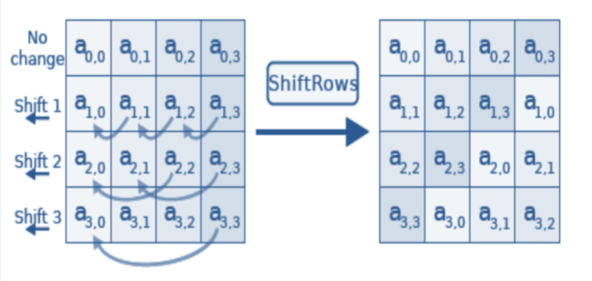

No change
Shift 1
Shift 2
Shift 3
ShiftRows
$a_{0,0}$ $a_{0,1}$ $a_{0,2}$ $a_{0,3}$
$a_{1,0}$ $a_{1,1}$ $a_{1,2}$ $a_{1,3}$
$a_{2,0}$ $a_{2,1}$ $a_{2,2}$ $a_{2,3}$
$a_{3,0}$ $a_{3,1}$ $a_{3,2}$ $a_{3,3}$
$a_{0,0}$ $a_{0,1}$ $a_{0,2}$ $a_{0,3}$
$a_{1,1}$ $a_{1,2}$ $a_{1,3}$ $a_{1,0}$
$a_{2,2}$ $a_{2,3}$ $a_{2,0}$ $a_{2,1}$
$a_{3,3}$ $a_{3,0}$ $a_{3,1}$ $a_{3,2}$

Figure 7. ShiftRows Schema

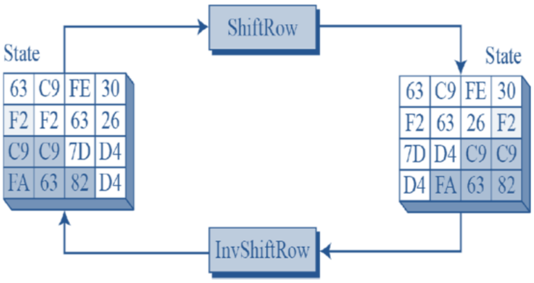
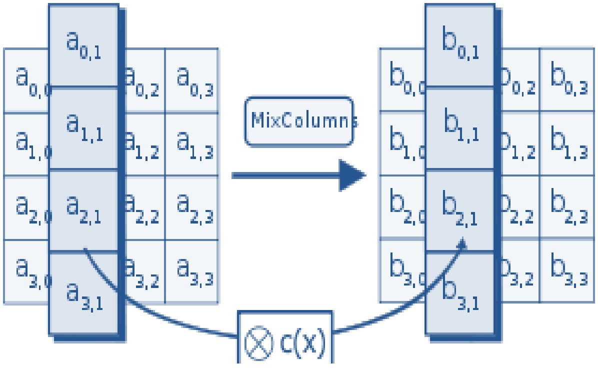


Figure 8. Inverse ShiftRows Schema

e) Mix Columns Operation

The Mix Columns step uses an invertible linear transformation to mix the four bytes of each column of the state. Mix Columns accepts four bytes as input and returns four bytes, with each input byte having an effect on all four output bytes. Mix Columns, in conjunction with ShiftRows, offers dispersion inside the cipher. Each column is multiplied by the known matrix for the 128-bit key during this process. ***Multiplication is defined as follows:*** When you do simple multiplications, there is no change. Multiplying by two causes a shift to the left. Multiplication by three additionally causes a shift to the left, but also does XOR (exclusive-or) with the upshifted original number. If the shifted value is larger than 0xFF after shifting, a conditional XOR with 0x1B should be performed, as shown in Fig.9. Alternatively, the Mix Columns step may be seen as a multiplication in a finite field by a particular MDS matrix. This technique is more thoroughly described in the article Rijndael column mix.

$$\begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix}.$$

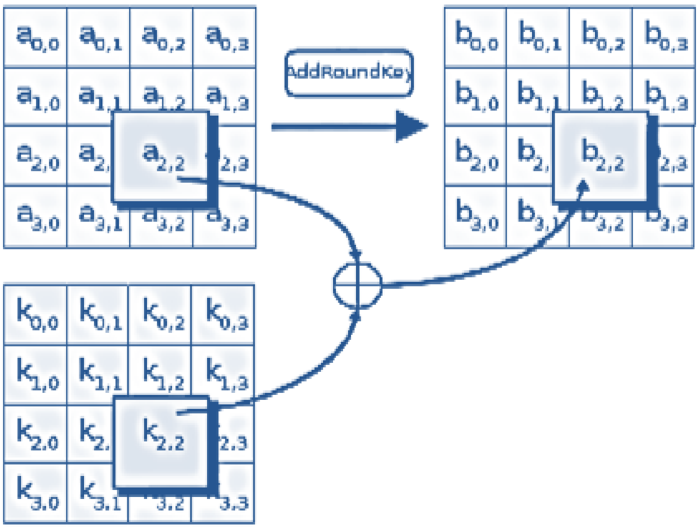


$a_{0,0}$ $a_{0,1}$ $a_{0,2}$ $a_{0,3}$
$a_{1,0}$ $a_{1,1}$ $a_{1,2}$ $a_{1,3}$
$a_{2,0}$ $a_{2,1}$ $a_{2,2}$ $a_{2,3}$
$a_{3,0}$ $a_{3,1}$ $a_{3,2}$ $a_{3,3}$
MixColumns
$\otimes c(x)$
$b_{0,0}$ $b_{0,1}$ $b_{0,2}$ $b_{0,3}$
$b_{1,0}$ $b_{1,1}$ $b_{1,2}$ $b_{1,3}$
$b_{2,0}$ $b_{2,1}$ $b_{2,2}$ $b_{2,3}$
$b_{3,0}$ $b_{3,1}$ $b_{3,2}$ $b_{3,3}$

Figure 9. Mix Columns

f) AddRoundKey Operation

A basic bitwise XOR is used to apply a Round Key to the state in this operation. By using the key schedule, the Round Key is generated from the Cipher Key. The length of the Round Key is identical to the length of the block key, which is 128 bits. Fig.10 depicts the AddRoundKey operation, which combines the subkey and the state.



$a_{0,0}$ $a_{0,1}$ $a_{0,2}$ $a_{0,3}$
$a_{1,0}$ $a_{1,1}$ $a_{1,2}$ $a_{1,3}$
$a_{2,0}$ $a_{2,1}$ $a_{2,2}$ $a_{2,3}$
$a_{3,0}$ $a_{3,1}$ $a_{3,2}$ $a_{3,3}$
AddRoundKey
$b_{0,0}$ $b_{0,1}$ $b_{0,2}$ $b_{0,3}$
$b_{1,0}$ $b_{1,1}$ $b_{1,2}$ $b_{1,3}$
$b_{2,0}$ $b_{2,1}$ $b_{2,2}$ $b_{2,3}$
$b_{3,0}$ $b_{3,1}$ $b_{3,2}$ $b_{3,3}$
$\oplus$
$k_{0,0}$ $k_{0,1}$ $k_{0,2}$ $k_{0,3}$
$k_{1,0}$ $k_{1,1}$ $k_{1,2}$ $k_{1,3}$
$k_{2,0}$ $k_{2,1}$ $k_{2,2}$ $k_{2,3}$
$k_{3,0}$ $k_{3,1}$ $k_{3,2}$ $k_{3,3}$

Figure 10. AddRoundKey Operation

g) DNA Swapping

The message is converted to a decimal format. Tab. 5 depicts the sequence of a DNA exchange operation with a key size of 3.

Table 4. DNA Rule (2)

DNA sequence
A=G, T=C
A=C, T=G
A=T, C=G

4. Results

In the experimental analysis, there are a range of security tests and their associated conclusions, such as key space and statistical analyses, numerical analyses, differential analyses, and encryption quality analyses, among other things. When it comes to verifying the suggested algorithm's acceptable security, these tests are the most important. Covid19-dataset is used in this work; Covid19-dataset is a massive and constantly developing collection of well-characterized digital recordings of X-rays images intended for use by the Kaggle "Google" research community, and it is used in this study.

4.1. Simulation Environment

The suggested method was simulated using a reputable simulation program, MATLAB version (2020a). The tests were conducted on a machine equipped with the following specifications:

Table 5. Simulation Machine Specifications

Model	Dell- Inspiron 5000
CPU	4GHz-Intel-Core-i7-5500U
CPU speed	3.40 GHz
Memory	16 GB

4.2. Time analysis for encryption and decryption

Calculating encryption and decryption throughput can be done using the encryption and decryption time. When it comes to X-ray images, the algorithm's performance criteria include the amount of time it takes to encrypt and decode. Therefore, it was repeated a total of ten times. Average of an experiment is a term used to describe the average of the ten outcomes of an experimental design.

Table 6. Encryption & decryption time with different rounds “299*299 X-Ray”

X-Ray Image	10 Round AES		2-rounds MLAESDNA		5-rounds MLAESDNA		10-rounds MLAESDNA	
	ET	DT	ET	DT	ET	DT	ET	DT
COVID-1.png	729.7	1253.8	132.6772	364.0475	325.0425	652.4034	613.678	1129.81
COVID-2.png	715.3	1230.7	143.6768	359.9231	351.9902	645.0121	664.555	1117.01
COVID-3.png	690.4	1140.3	131.7603	347.3501	322.7962	622.4802	609.437	1077.99
COVID-4.png	650.8	1103.4	127.7294	340.1646	312.9212	609.6032	590.793	1055.69
COVID-5.png	632.3	1050.5	123.8288	359.153	303.365	643.632	572.751	1114.62

** ET, DT =Encryption Time in second & Decryption Time in second*

4.3. Security analysis

The security of the encryption approach that has been proposed has been thoroughly investigated. To determine a cipher's resistance to various types of attacks, a variety of security analysis methodologies are employed. When determining the resistance of a system to a brute force attack, the key space analysis technique is employed. To determine statistical attack resistance, the histogram, Correlation Analysis of Adjacent Values, and Correlation Analysis of Original and Encrypted X-Ray Images are all employed in conjunction with each other. In mathematics, for example, entropy is a measure of unpredictability that may be calculated. When evaluating the effectiveness of applied focus measures on the quality of X-Ray images, the MSE was utilized to determine their effectiveness.

4.4. Keyspace analysis

The suggested method was compared to previous efforts, and the findings indicate that it would take (5.179340*1027) years to break or hack the proposed algorithm. Tab.8 demonstrates that the proposed method provides superior security against brute-force attacks and requires a significant amount of time to crack when compared to previous studies.

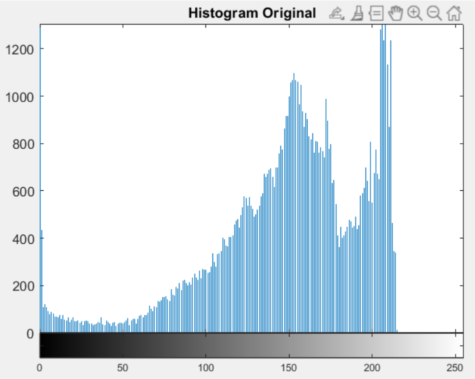
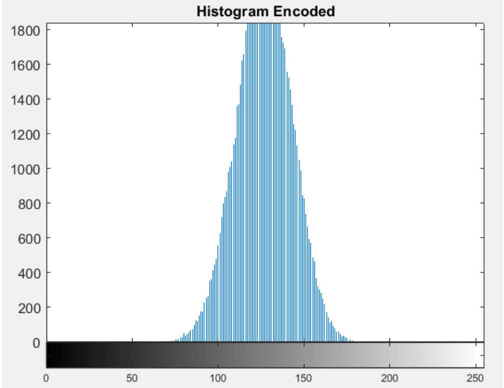
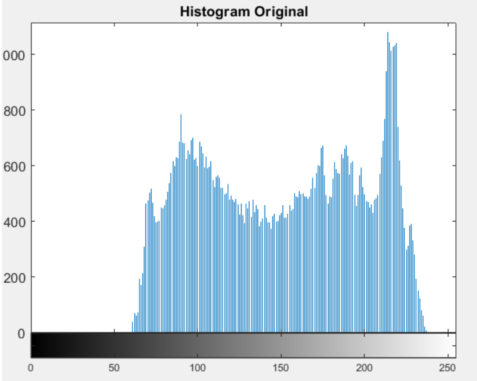
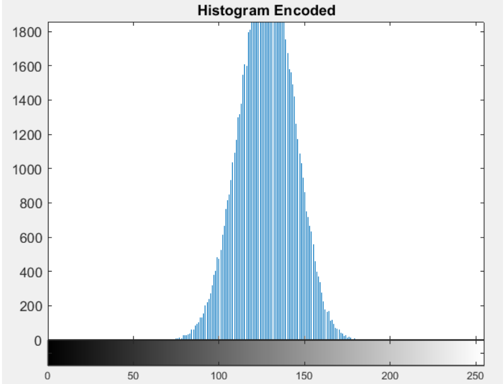
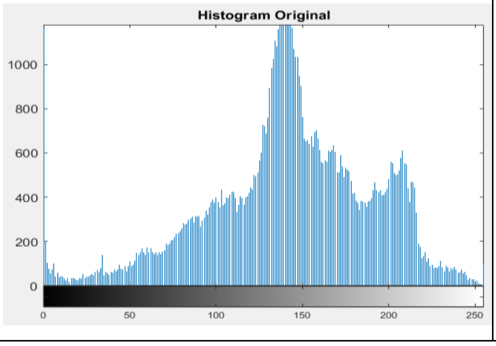
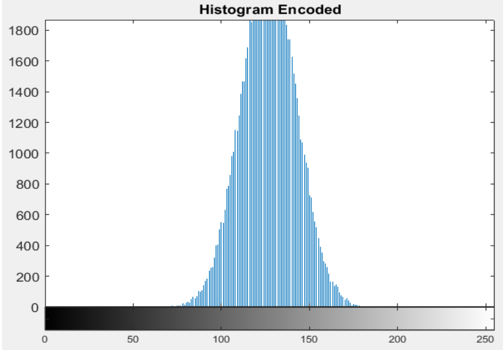
Table 7. Decryption breaking time

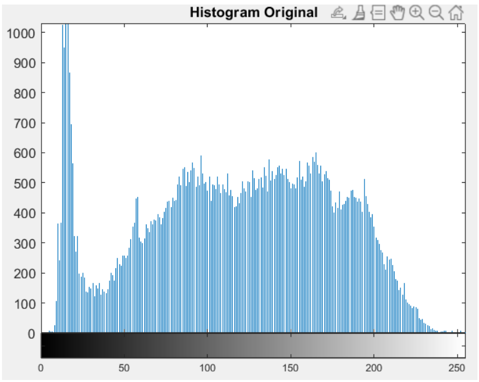
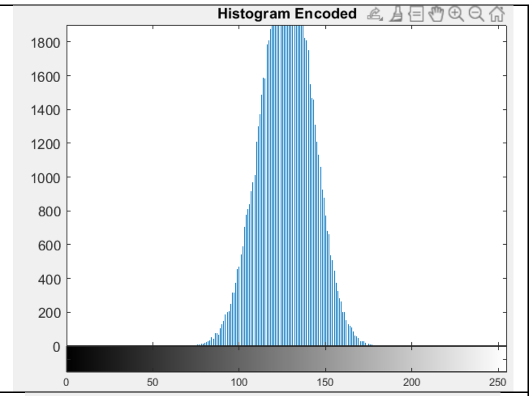
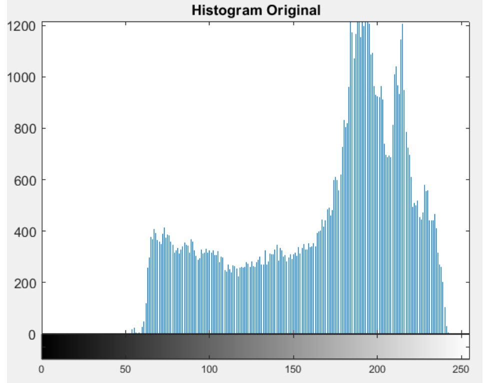
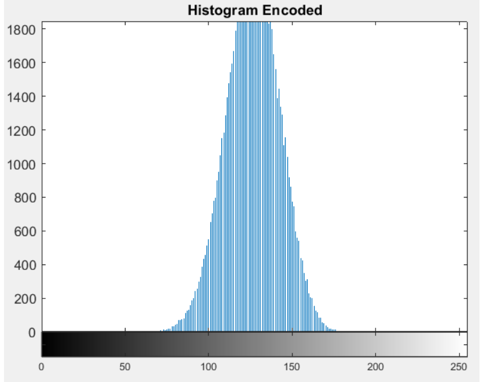
	Keyspace	**Key-Length (bits)**	**Breaking Time (years)**
LEA: [32]	2^{128}	128	$1.078950 * 10^{25}$
Original AES	2^{128}	128	$1.078950 * 10^{25}$
MLAESDNA	$2^4 *2^{128} *3*10$	4*128*3*10	$\mathbf{5.179340 * 10^{27}}$

4.5. Histogram analysis

The suggested method was tested on a variety of X-ray images. Tab.9 demonstrates that the cipher X-ray's histograms are very uniform and substantially different from the plain X-ray's histograms, which makes statistical analysis assaults on the encrypted x-ray extremely difficult.

Table 8: Histograms (Original and Encrypted Covid 19 image dataset).

X-Ray	Original Image	Cipher Image
COVID-1.png		
COVID-2.png		
COVID-3.png		

COVID-4.png		
COVID-5.png		

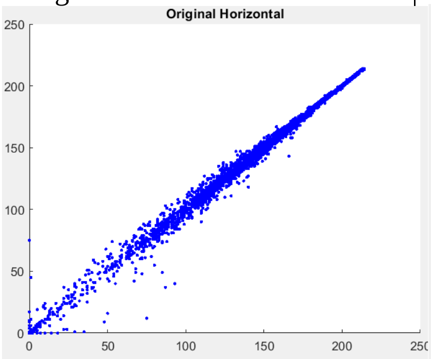
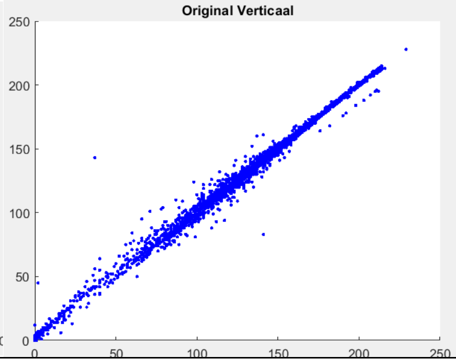
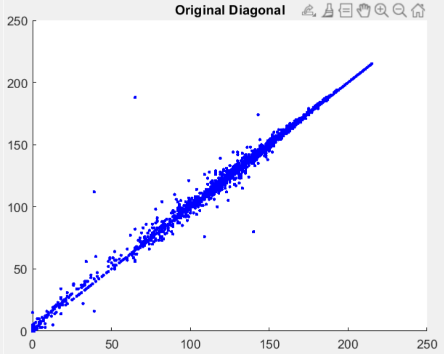
4.6. Correlation analysis

To determine the cryptosystem's efficiency, the correlation between two consecutive values is evaluated in both plain and cipher X-ray pictures. The method is as follows. To begin, a random selection of 50 pairs of adjacent values (horizontal, vertical, and diagonal) from the original X-ray pictures and the encrypted X-ray images is made. The correlation coefficient for each pair is then determined [33]. Tab. 10 illustrates the horizontal, vertical, and diagonal distribution of neighboring pixel pairs in the plain X-ray pictures and their cipher X-ray images. The pixel pairings in the simple Covid 19 picture dataset are mainly clustered around the graph's diagonal line. Tab. 11 illustrates The correlation between Original image and cipher-image. Correlation coefficients between the original and encrypted pictures may be computed using the following formula:

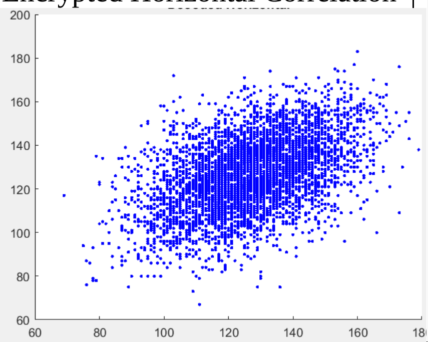
$$\rho = \frac{\sum_{i=1}^{n}\sum_{i=1}^{m}(X(i,j)-E(X))\,(Y(i,j)-E(Y))}{\sqrt{\sum_{i=1}^{n}\sum_{i=1}^{m}(X(i,j)-E(X))^2\ \sum_{i=1}^{n}\sum_{i=1}^{m}(Y(i,j)-E(Y))^2}} \qquad (1)$$

Where, *X (i, j), Y (i, j)* are the i_{th} row and j_{th} column pixel values of X-Ray image and encrypted image respectively. *E (X), E (Y)* represent the average of X-Ray image and encrypted image respectively. *(n, m)* is the image dimension [38] [37].

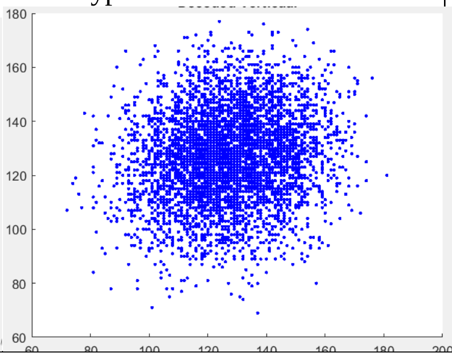
Table 9. Correlations of Original and Encrypted X-ray images

COVID-1.png		
Original Horizontal Correlation	Original Vertical Correlation	Original Diagonal Correlation
		

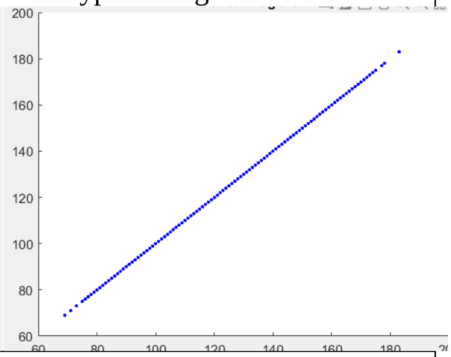
Encrypted Horizontal Correlation



Encrypted Vertical Correlation

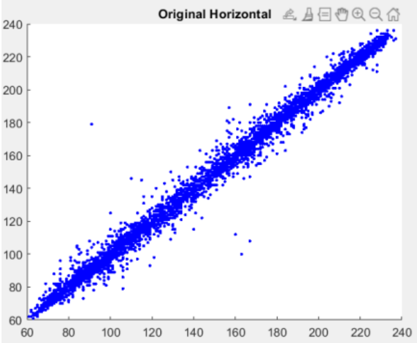


Encrypted Diagonal Correlation

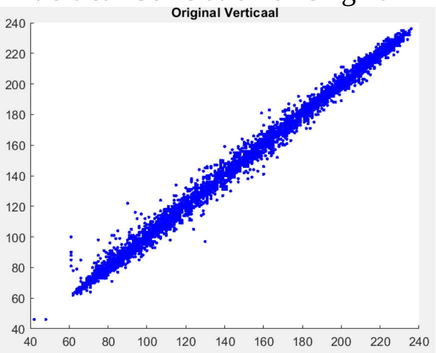


COVID-2.png

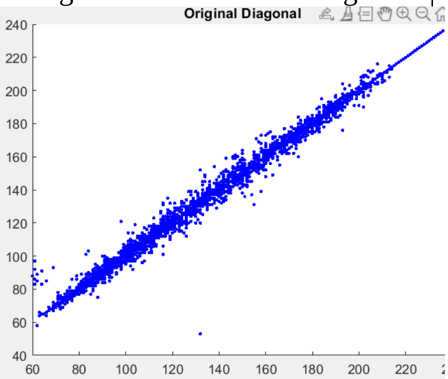
Original Horizontal Correlation



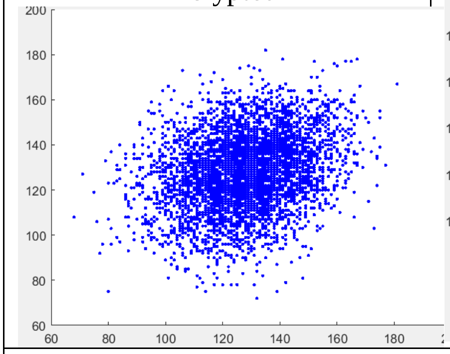
Vertical Correlation of Original



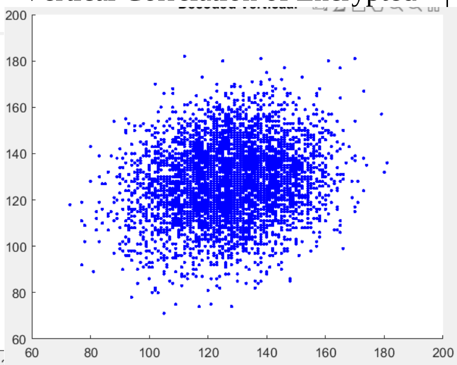
Diagonal Correlation of Original



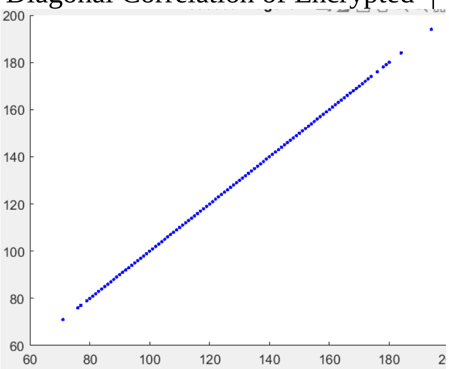
Horizontal Correlation of Encrypted



Vertical Correlation of Encrypted

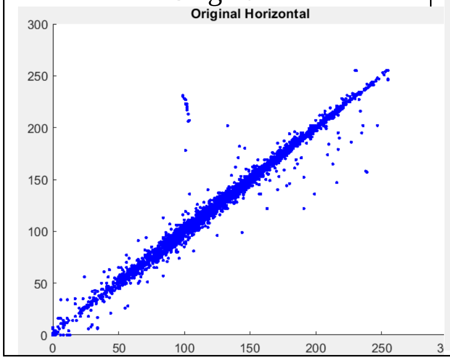


Diagonal Correlation of Encrypted

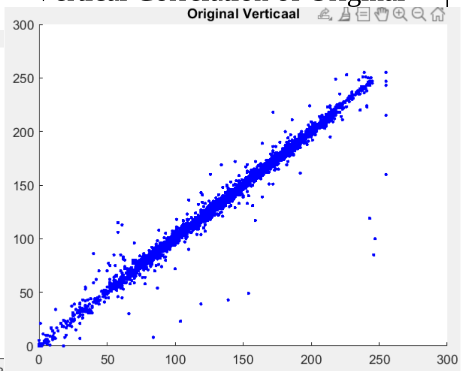


COVID-3.png

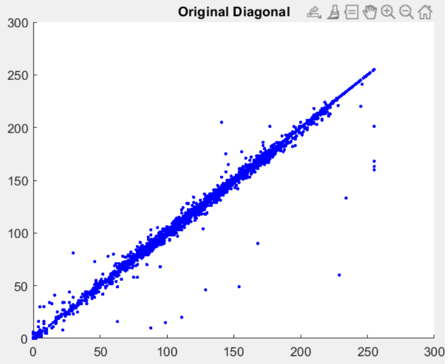
Horizontal Correlation of Original

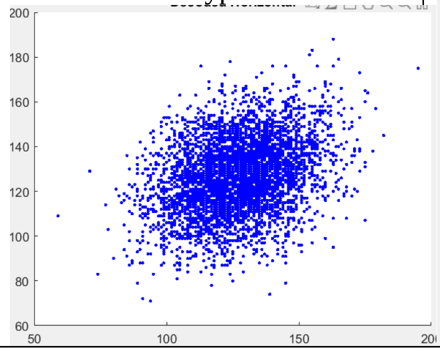
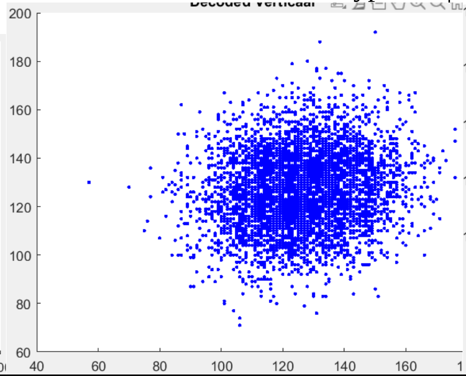
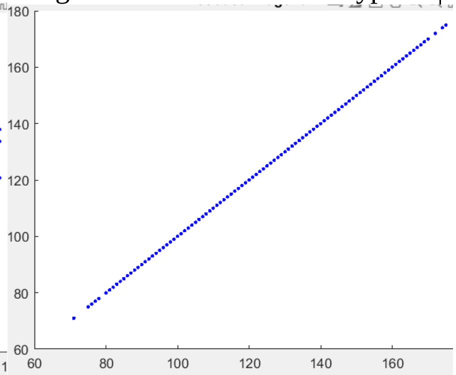
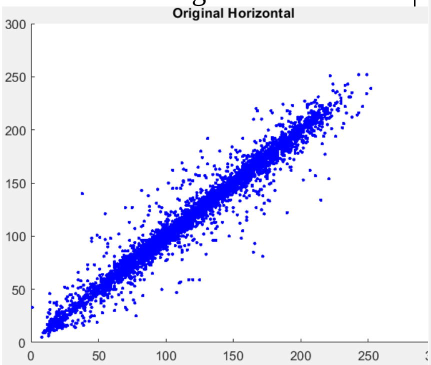
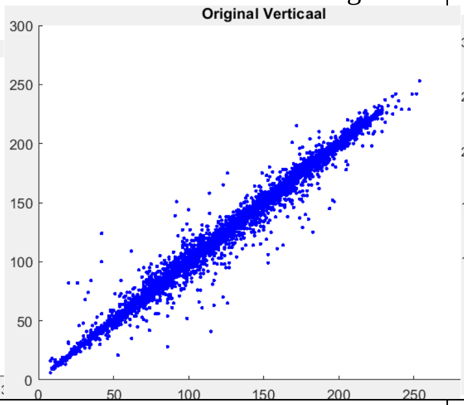
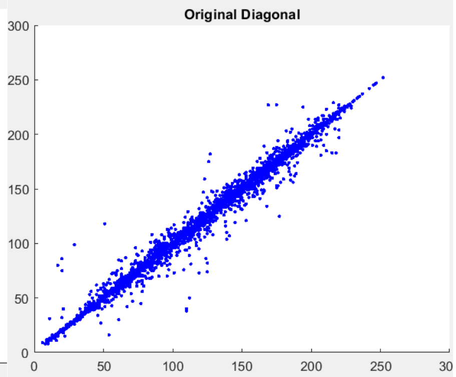
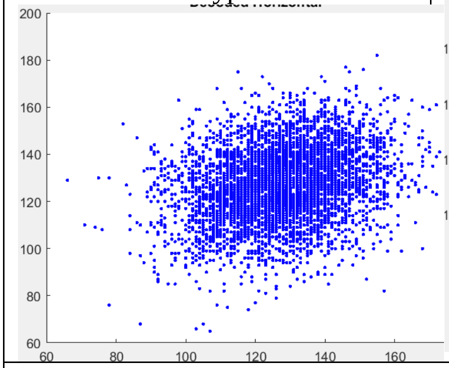
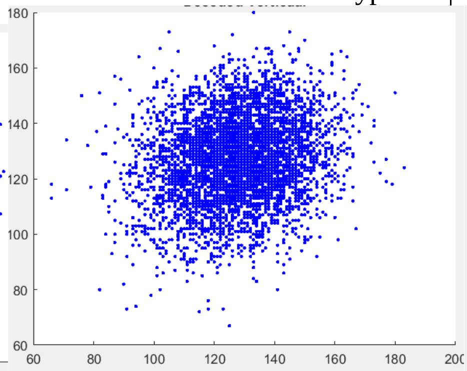
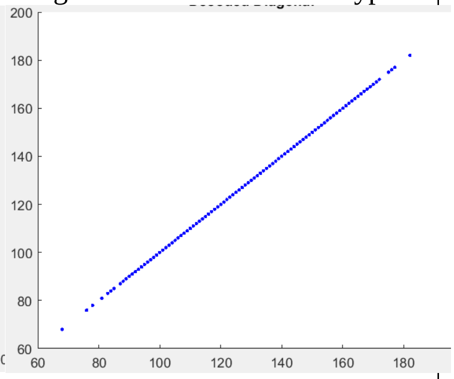
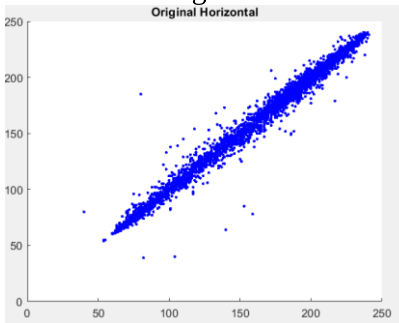
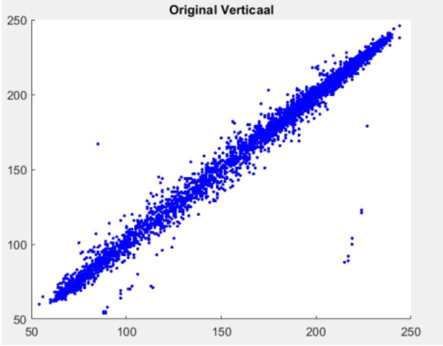
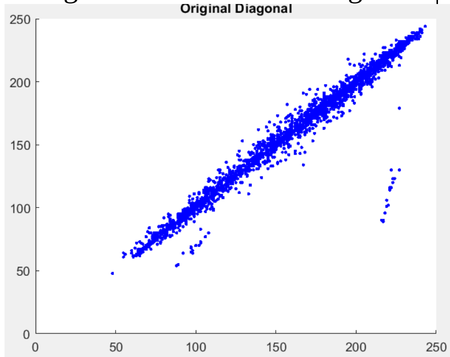


Vertical Correlation of Original



Diagonal Correlation of Original



Horizontal Correlation of Encrypted 	Vertical Correlation of Encrypted 	Diagonal Correlation of Encrypted 
COVID-4.png		
Horizontal Correlation of Original 	Vertical Correlation of Original 	Diagonal Correlation of Original 
Horizontal Correlation of Encrypted 	Vertical Correlation of Encrypted 	Diagonal Correlation of Encrypted 
COVID-5.png		
Horizontal Correlation of Original 	Vertical Correlation of Original 	Diagonal Correlation of Original 

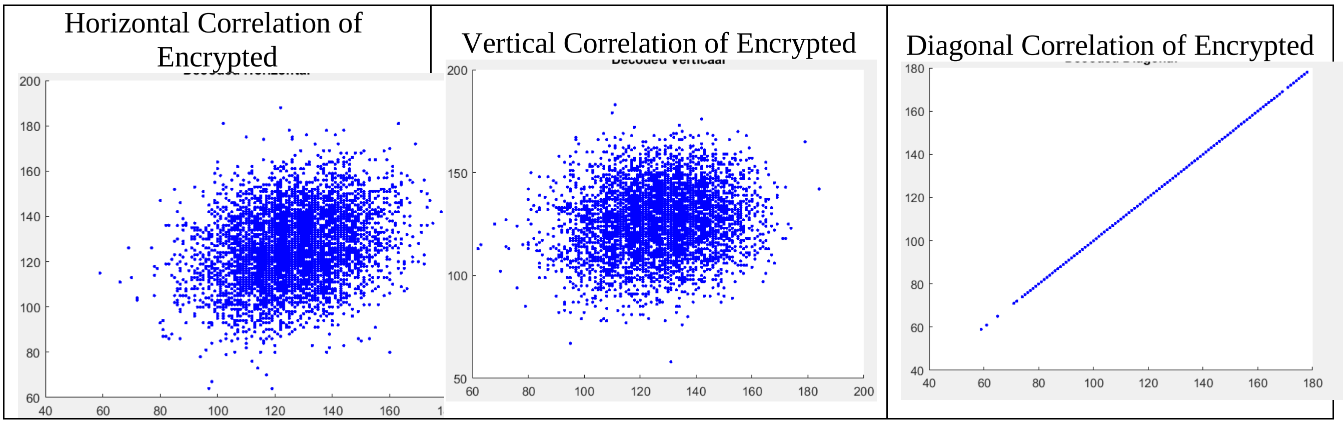


Table 11. The correlation between original image and cipher-image

Covid 19 image Name	AES	MLAESDNA
COVID-1.png	-0.0121178	-0.0231638
COVID-2.png	-0.0034151	-0.0204151
COVID-3.png	**0.0536818**	**0.0236818**
COVID-4.png	-0.00199972	-0.0188972
COVID-5.png	0.00161543	0.00521543

4.7. Entropy analysis and differential analysis metrics

Randomness and uncertainty are key characteristics of a Covid 19 picture and the Entropy is frequently employed to assess the pixel-level uniform distribution of gray-levels in these images. At equilibrium, the entropy is near to 8, thus the diffusion process yields high-order disorganization at the output [34-36]. Tab.21 displays the entropy information of the encrypted Covid 19 picture collection. These findings show that the cipher Covid 19 image dataset's information entropy is near to ideal, confirming that the suggested Algorithm's cipher Covid 19 image has a fair amount of unpredictability.

Differential analysis, or differential attack, is one of the most frequently used cryptanalysis techniques for iterated block ciphers [39]. Two widely used quantitative measures, the Number of Pixels Change Rate (NPCR) and the Unified Average Changing Intensity (UACI), are used to assess an algorithm's sensitivity to a small change in the input picture. The findings of NPCR and UACI are summarized in Table 4.7. The NPCR value of a genuine random cipher image should ideally be near to 100%, whereas the higher value of the UACI test estimates the average intensity difference between a plain picture and a cipher image, which is anticipated to be close to 33% as stated in [40] [41]. The findings indicate that the NPCR and UACI values for all test pictures are very close to the theoretical values, indicating that the proposed method is highly resistant to differential attack. These findings are directly linked to the suggested algorithm's high degree of confusion and dispersion.

Entropy is a critical element of randomness and system complexity measurement. Increased entropy indicates that the system is more complicated. The entropy of information is computed as [42] [38]:

$$H(s) = \sum_{i} p(s_i)\ \log 2\ \frac{1}{p(s_i)} \tag{2}$$

where s_i denotes the gray-level and $p(s_i)$ denotes the probability of the occurrence s_i. For gray scale pictures where the image pixels are regarded random occurrences, the optimum entropy value is 8, and therefore the image with the closest value to 8 has the lowest degree of uncertainty [42] [38].

Differential analysis is a method that is used to determine the encryption algorithm's resistance to differential attack [39]. Two widely used quantitative measures, the Number of Pixels Change Rate (NPCR) and the Unified Average Changing Intensity (UACI), are used to assess an algorithm's sensitivity to a small change in the input picture. NPCR is a technique for determining the percentage of different pixel values between two pictures and may be computed as:

$$NPCR = \frac{\sum_{i=1}^{w}\sum_{i=1}^{h} D(i,j)}{w * h} * 100\% \tag{3}$$

The UACI algorithm is used to determine the average intensity of a variety of pictures. The UACI is computed in the following manner:

$$UACI = \frac{1}{w * h} * \frac{\sum_{i=1}^{w}\sum_{i=1}^{h} |C1(i,j) - C2\ (i,j)|}{255} * 100\% \tag{4}$$

in this case, *C 1* and *C 2* are the two encrypted-images whose corresponding X-Ray image have only one-pixel difference, the gray-scale values of the pixels at position *(i, j)* of *C 1* and *C 2* are denoted as *C 1 (i, j)* and *C 2 (i, j)*, respectively; *W* and *H* are the width and height of *C 1* or *C 2*; *D(i, j)* is determined by *C 1(i, j)* and *C 2(i, j)*, namely, if *C 1 (i, j) = C 2 (i, j)* then *D(i, j)* = 0 otherwise, *D(i, j)* = 1.

Table 10. Results of Entropy, SSIM, NPCR and UACI of Original and Encrypted image dataset

	Entropy		**SSIM**		**NPCR**		**UACI**	
	AES	MLAESDNA	**AES**	MLAESDNA	**AES**	MLAESDNA	**AES**	MLAESDNA
COVID-1.png	5.5336	6.18014	0.02220	0.218729	0.99745	0.993758	0.310999	0.183976
COVID-2.png	5.6843	6.36434	0.12320	0.240833	0.99125	0.994228	0.336559	0.186948
COVID-3.png	5.4789	7.45646	0.36520	0.231926	0.99345	0.991219	0.312299	0.167165
COVID-4.png	5.9876	6.65581	0.36220	0.218864	0.99565	0.994575	0.333999	0.198113
COVID-5.png	5.1452	6.27741	0.03333	0.232261	0.99785	0.996801	0.344499	0.227581

4.8. Structural Content (SC), Normalized Absolute Error (NAE), Peak Signal-to-Noise Ratio (PSNR) and Mean Square Error (MSE) Analysis

It is defined as the product of the sum of the original image's pixel square values and the sum of the decrypted image's pixel square values. Additionally, it determines the connection between pictures. A lower SC value indicates a better level of quality; if there is no distortion in the encrypted pictures, SC equals 1 [43]. SC is computed as follows:

$$SC = \frac{\sum_{i=1}^{m}\sum_{i=1}^{n} f(i,j)^2}{\sum_{i=1}^{m}\sum_{i=1}^{n} \bar{f}(i,j)^2} \tag{5}$$

It is defined as the difference between the original picture f (i, j) and the decrypted image f' (i, j) divided by the total of the original image's pixel square value [44]. The NAE is computed in the following manner:

$$NAE = \frac{\sum_{i=1}^{m}\sum_{i=1}^{n} \| f(i,j)^2 - f'(,j)^2 \|}{\sum_{i=1}^{m}\sum_{i=1}^{n} f(i,j)^2} \tag{6}$$

It is calculated by dividing the square of the image's peak value by the Mean Square Error. The PSNR is used to quantify the quality of a grayscale picture after reconstruction [44] [45]. PSNR and MSE are computed as follows:

$$PSNR\ = 10 * \ log_{10}\left(\frac{255 * 255}{MSE}\right)\ (bB) \tag{7}$$

$$MSE = \frac{1}{mn}\sum_{i=1}^{m}\sum_{j=1}^{n} ||I_1(i,j) - I_2(i,j)||^2 \tag{8}$$

The mean square error between the decrypted image I2 (i, j) and the original image is denoted by MSE I1(i, j). m and n indicate the original image's width and height, respectively [44] [45].

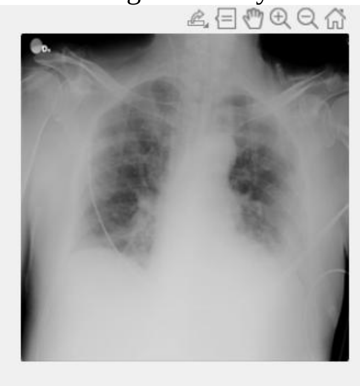
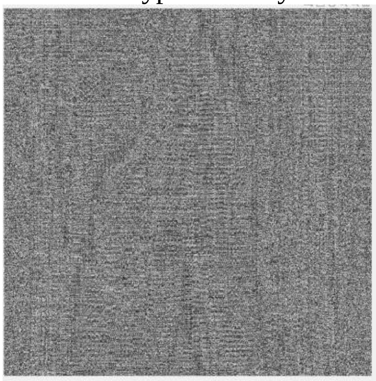
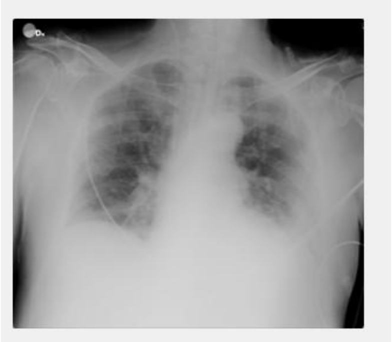
Tab. 13 shows the PSNR, MSE, NAE, and SC statistical measures that were utilized to assess the proposed method. The difference between the original Covid 19 picture and the encrypted Covid 19 image is represented by the value of metrics.

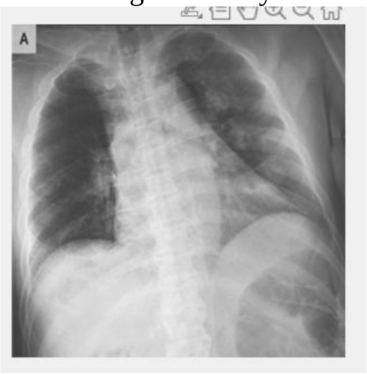
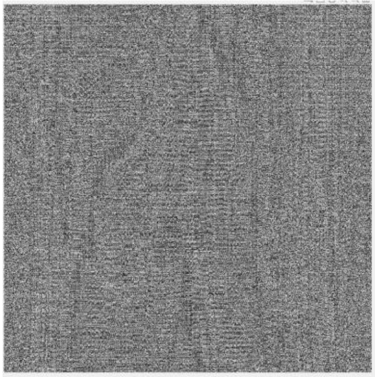
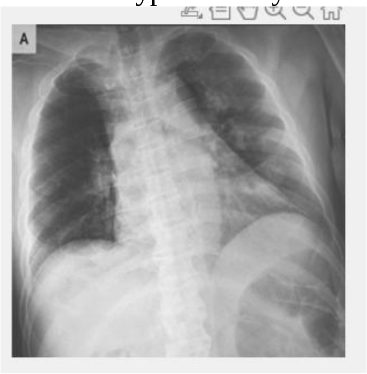
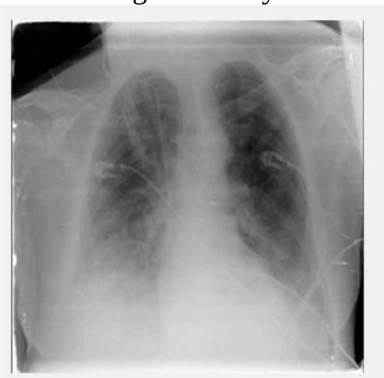
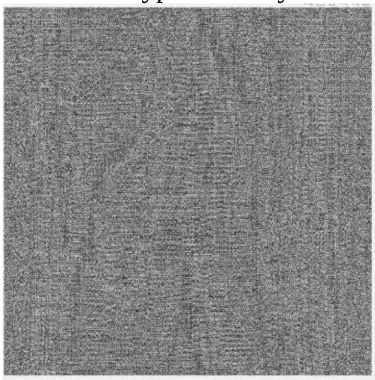
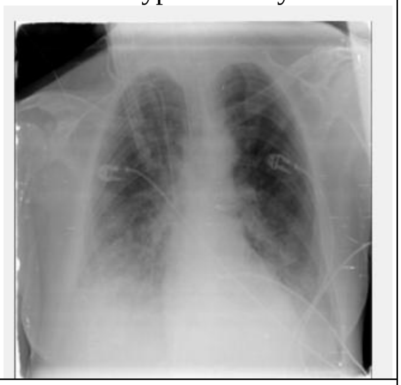
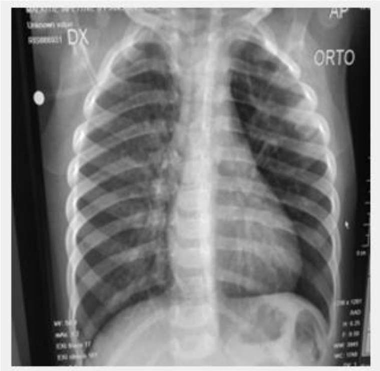
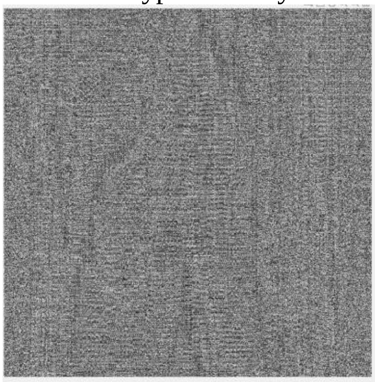
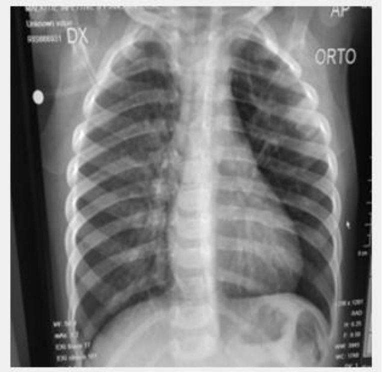
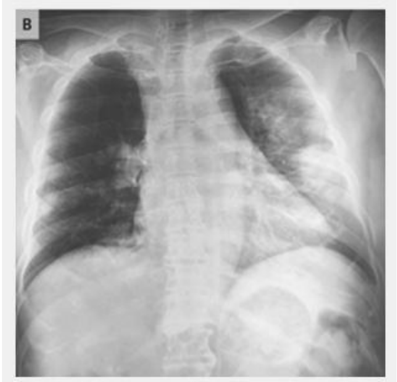
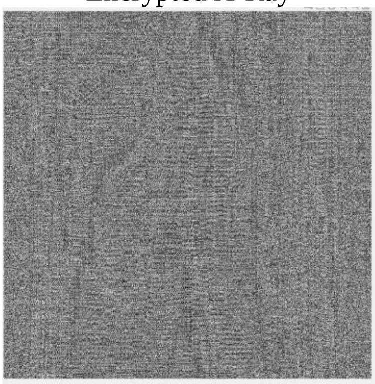
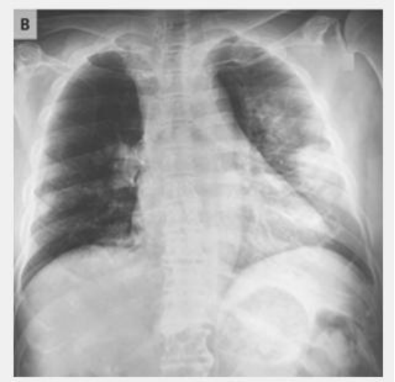
Table 11. MSE of "Signal Length=1000"

	PSNR	**MSE**	**NAE**	**SC**
	AES& MLAESDNA	AES& MLAESDNA	AES& MLAESDNA	AES& MLAESDNA
COVID-1.png	Inf	0	0	1
. . .				
COVID-n.png				

Any encryption technique's primary concern is security. A strong encryption algorithm should be resistant to the majority of known attacks. The key space analysis technique is used to determine the resistance of a system to brute force assault. The key space in the proposed method is (24*2128*3*10). This is more than the effective key size required to guarantee computational security against future brute force assaults. It was shown that the histograms of the ciphered Covid 19 picture dataset are markedly different from those of the original Covid 19 image dataset, implying that statistical cryptanalysis on the ciphered Covid 19 image is very difficult. Correlation coefficients reveal that the value distribution of the encryption Covid 19 image dataset is distorted significantly in terms of correlation between values. As a result, value information cannot be derived from neighboring values. Additionally, the information entropies of the cipher Covid 19 image dataset are near to the ideal value, indicating that the proposed algorithm's cipher Covid 19 picture has a high degree of unpredictability. As a result, the suggested method is impervious to differential attack. These findings are obtained as a consequence of the suggested algorithm's powerful process of confusion and dispersion. The MSE is used to assess the effectiveness of focus measures that have been applied. The suggested method achieves much better outcomes. Experiments and results of different statistical metrics have shown that the suggested method is resistant to traditional forms of assault. Tab.10: Original, Encrypted and Decrypted X-ray Image Samples.

Table 12. Original, Encrypted and Decrypted X-ray image Samples

COVID-1.png		
Original X-Ray 	Encrypted X-Ray 	Decrypted X-Ray 

<table>
<tr><td colspan="3"><b>COVID-2.png</b></td></tr>
<tr><td>Original X-Ray
 </td><td>Encrypted X-Ray
</td><td>Decrypted X-Ray
 </td></tr>
<tr><td colspan="3"><b>COVID-3.png</b></td></tr>
<tr><td>Original X-Ray
</td><td>Encrypted X-Ray
</td><td>Decrypted X-Ray
</td></tr>
<tr><td colspan="3"><b>COVID-4.png</b></td></tr>
<tr><td>Original X-Ray
 </td><td>Encrypted X-Ray
</td><td>Decrypted X-Ray
 </td></tr>
<tr><td colspan="3"><b>COVID-5.png</b></td></tr>
<tr><td>Original X-Ray
 </td><td>Encrypted X-Ray
</td><td>Decrypted X-Ray
 </td></tr>
</table>

The histogram analysis, the correlation between nearby data, the entropy analysis, and the MSE analysis all show that MLAESDNA is statistically resistant. These findings are linked to the great sensitivity of the three distinct keys and the high degree of randomness inherent in DNA computing.

5. Conclusion

This study demonstrated a multi-layer encryption method based on DNA computing and the AES algorithm MLAESDNA. Increased key length offers a number of benefits in IoT, particularly in medical health systems, since it reduces the size of the Covid-19 X-Ray picture, which reduces the need for complicated mathematical calculations that use more resources and take longer to complete. MLAESDNA makes advantage of the four keys provided by DNA Rules. This increases the encryption strength and complexity of MLAESDNA. The necessary decryption time is raised by more than 48 times compared to the original method. By integrating the AES and DNA computing concepts, we were able to significantly improve the encryption/decryption procedures. The findings indicated that MLAESDNA outperformed the original AES algorithm and many other methods. According to the results of the tests, MLAESDNA has a high degree of security, integrity, efficiency, and resilience. MLAESDNA satisfies the criteria for transmitting the Covid 19 image collection over unsecure healthcare system channels. By and large, the field of cooperative encryption is ripe for study. The goal of future work is to accelerate encryption and decryption execution times by combining quantum computing concepts with MLAESDNA, to implement MLAESDNA using parallel processing, and to apply MLAESDNA to all medical signals in industry.

6. Acknowledgement

The authors would like to thank BIOCORE Research Group, Faculty of Information and Communication Technology, Universiti Teknikal Malaysia Melaka.

References

[1] V. Muthukumaran, I. Manimozhi, P.S. PV, T. Karthikeyan, and M. Gopu, "Public Key Encryption With Equality Test for Industrial Internet of Things Based on Near-Ring". *International Journal of e-Collaboration (IJeC)*, *17*(3), pp.25-45, 2021.

[2] D. Choudhary, and R. Pahuja, "Encryption Techniques for Intelligent Transportation Systems via Deep Learning for IOV in Smart Cities", 2021.

[3] R. Hanumantharaju, D.P. Kumar, B.J. Sowmya, G.M. Siddesh, K.N. Shreenath, and K.G. Srinivasa, "Enabling Technologies for Fog Computing in Healthcare 4.0: Challenges and Future Implications", In *Fog Computing for Healthcare 4.0 Environments* (pp. 157-176). Springer, Cham, 2021.

[4] T.H. Jo, J.H. Ma, and S.H. Cha, "Elderly Perception on the Internet of Things-Based Integrated Smart-Home System", *Sensors*, *21*(4), p.1284, 2021.

[5] I. Ahmad, X. Liao, and S. Nazir, "Evaluation and Quality Assurance of Fog Computing-Based IoT for Health Monitoring System. *Wireless Communications and Mobile Computing*, *2021*.

[6] A. A. Mutlag, M. Khanapi Abd Ghani, , M. A. Mohammed, M. S. Maashi et al. "MAFC: Multi-Agent fog computing model for healthcare critical tasks management", *Sensors*, vol. 20, no. 7, p.1853, 2020.

[7] N. Gupta, S. Gupta, M. Khosravy, N. Dey, N. Joshi, R.G. Crespo, and N. Patel, "Economic IoT strategy: the future technology for health monitoring and diagnostic of agriculture vehicles". *Journal of Intelligent Manufacturing*, *32*(4), pp.1117-1128, 2021.

[8] K. H. Abdulkareem, M. A. Mohammed, S. S. Gunasekaran, M. N. Al-Mhiqani, A. A. Mutlag et al, “A review of fog computing and machine learning: Concepts, applications, challenges, and open issues,” *IEEE Access*, vol. 7, pp. 153123–153140, 2019.

[9] A. Chacko and T. Hayajneh, “Security and privacy issues with iot in healthcare,”, *EAI Endorsed Transactions on Pervasive Health and Technology*, vol. 4, no. 14, 2018.

[10] K. Muhammad, M.S. Obaidat, T. Hussain, J.D. Ser, N. Kumar, M. Tanveer, and F. Doctor, "Fuzzy Logic in Surveillance Big Video Data Analysis: Comprehensive Review, Challenges, and Research Directions". *ACM Computing Surveys (CSUR)*, *54*(3), pp.1-33, 2021.

[11] G. Kaur, K. Singh, and H.S. Gill, "Chaos-based joint speech encryption scheme using SHA-1". *Multimedia Tools and Applications*, *80*(7), pp.10927-10947, 2021.

[12] B. M. Krishna, H. Khan, G. L. Madhumati, B. Lohitha, E. Bhavitha et al, “FPGA implementation of

DNA based AES algorithm for cryptography applications," *International Journal of Pure and Applied Mathematics*, vol. 115, no. 7, pp. 525-530, 2017.

[13] S. Kalsi, H. Kaur and V. Chang, "DNA cryptography and deep learning using genetic algorithm with NW algorithm for key generation," *Journal of Medical Systems*, vol. 42, no. 1, Jan. 2018.

[14] M. Sabry, M. Hashem, T. Nazmy and M. E. Khalifa, "Design of DNA-based advanced encryption standard (AES)", *IEEE Seventh International Conference on Intelligent Computing and Information Systems (ICICIS)*, IEEE. pp. 390-397 , 2015.

[15] H. M. Bahig and D. I. Nassr, "DNA-based AES with silent mutations," *Arabian Journal for Science and Engineering*, vol. 44, no. 4, pp. 3389–3403, Apr. 2019.

[16] A. H.Al-Wattar, R. Mahmod, Z. A. Zukarnain and N. Udzir, "A new DNA based approach of generating key dependent mix columns transformation," *International Journal of Computer Networks & Communications*, vol. 7, no. 2, pp. 93–102, Mar. 2015.

[17] P. Deshmukh and V. Kolhe, "Modified AES based algorithm for MPEG video encryption.," *ICICES2014 - S.A.Engineering College, Chennai*, pp. 1-5, 2014.

[18] P. M. Chanal and M. S. Kakkasageri, "Hybrid algorithm for data confidentiality in Internet of Things", *10th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, IEEE. pp. 1-5, 2019.

[19] G. Singh, "A Paper of encryption algorithms (RSA, DES, 3DES and AES) for information security", *International Journal of Computer Applications*. vol. 67, no. 19, 2013.

[20] N. Drucker, S. Gueron and V. Krasnov, "Making AES great again: the forthcoming vectorized AES instruction", *16th International Conference on Information Technology-New Generations (ITNG 2019)*, Springer, Cham, pp. 37-41, 2019.

[21] M. M. Wong, M. L. D. Wong, C. Zhang and I. Hijazin, "Circuit and system design for optimal lightweight AES encryption on FPGA", *Nanyang Technological University, Singapore*, 2018.

[22] P. Dixit, A. K. Gupta, M. C. Trivedi and V. K. Yadav, "Traditional and hybrid encryption techniques: A Survey", *In Networking Communication and Data Knowledge Engineering*, pp. 239–248, 2018.

[23] A. Ibrahim and G. Dalkiliç, "An advanced encryption standard powered mutual authentication protocol based on elliptic curve cryptography for RFID, proven on WISP," *Journal of Sensors*, 2017.

[24] S. Panghal, S. Kumar and N. Kumar, "Enhanced security of data using image steganography and AES encryption technique", *International Journal of Computer Applications*, vol. 42. 2016.

[25] M. A. Albahar, O. Olawumi, K. Haataja and P. Toivanen, "Novel hybrid encryption algorithm based on AES, RSA, and Twofish for bluetooth encryption," *Journal of Information Security.*, vol. 09, no. 02, pp. 168–176, 2012.

[26] P. Kumar and S. B. Rana, "Development of modified AES algorithm for data security," *Optik (Stuttg).*, vol. 127, no. 4, pp. 2341–2345, Feb. 2016.

[27] Q. Zhang and A. Qunding, "Digital image encryption based on Advanced Encryption Standard(AES) algorithm," *in Proceedings - 5th International Conference on Instrumentation and Measurement, Computer, Communication, and Control, IMCCC 2015*, pp. 1218–1221, 2016.

[28] M. A. Khan and K. Salah, "IoT security: Review, blockchain solutions, and open challenges," *Future Generation Computer Systems*, vol. 82, pp. 395–411, May 2018.

[29] L. Cardelli, "Two-domain DNA strand displacement," *Electronic Proceedings in Theoretical Computer Science*, vol. 26, pp. 47–61, Jun. 2010.

[30] S. Namasudra and G. C. Deka, "Advances of DNA computing in cryptography*", In Advances of DNA computing in cryptography*, 2018.

[31] M. Elhoseny, G. Ramírez-González, O. M. Abu-Elnasr, S. A. Shawkat, N. Arunkumar et al, "Secure medical data transmission model for IoT-based healthcare systems," *IEEE Access*, vol. 6, pp. 20596–20608, Mar. 2018.

[32] H. M. El Hennawy, , A. E. Omar and S. M. Kholaif, "Design of LEA: Link encryption algorithm new proposed stream cipher algorithm", *31st National Radio Science Conference (NRSC), IEEE* , pp. 82-91, 2014.

[33] J. Wu, X. Liao and B. Yang, "Image encryption using 2D Hénon-Sine map and DNA approach," *Signal Processing*, vol. 153, pp. 11–23, Dec. 2018.

[34] X. J. Tong, M. Zhang, Z. Wang and J. Ma, "A joint color image encryption and compression scheme based on hyper-chaotic system," *Nonlinear Dynamics*, vol. 84, no. 4, pp. 2333–2356, Jun. 2016.

[35] T. Xiang, K. W. Wong and X. Liao, "Selective image encryption using a spatiotemporal chaotic system,"

Chaos, vol. 17, no. 2, 2007.

[36] R. Enayatifar, A. H. Abdullah, I. F. Isnin, A. Altameem and M. Lee, “Image encryption using a synchronous permutation-diffusion technique,” *Optics and Lasers in Engineering.*, vol. 90, pp. 146–154, Mar. 2017.

[37]. T. Xiang, K. Wong, and, X. Liao, “Selective Image Encryption using A Spatiotemporal Chaotic System”, Chaos: An Interdisciplinary Journal of Nonlinear Science, vol. 17, no. 2, pp. 1-13, 2007.

[38]. R. Enayatifar, A. Abdullah, I. Isnin, A. Altameem, and, M. Lee, “Image Encryption using A Synchronous Permutation - Diffusion Technique”, Optics and Lasers in Engineering, vol. 90, pp. 146-154, 2017.

[39]. M. Hamdi, R. Rhouma, and, S. Belghith, “A Selective Encryption-Encryption of Images Based on SPIHT Coding and Chirikov Standard Map”, Signal Processing, vol. 131, pp. 514-526, 2016.

[40]. M. Escobar, C. Hernández, F. Abundiz, R. Gutiérrez, and, O. Campo, “A RGB Image Encryption Algorithm Based on Total Plain Image Characteristics and Chaos,” Signal Processing, vol. 109, pp. 119-131, 2015.

[41]. S. Agarwal, “Secure Image Transmission Using Fractal and 2D-Chaotic Map,” Journal of Imaging, vol. 4, no. 1, p. 17, 2018.

[42]. X. Tong, M. Zhang, Z. Wang, and, J. MA, “A Joint Color Image Encryption and Compression Scheme Based on Hyper-Chaotic System”, Nonlinear Dynamics, vol. 84, no.4, pp. 2333-2356, 2016.

[43]. N. Nandy, D. Banerjee, and, C. Pradhan, “Color Image Encryption Using DNA Based Cryptography,” International Journal of Information Technology, pp. 1-8, 2018.

[44]. M. Elhoseny, G. Ramirez-Gonzalez, O. M. Abu-Elnasr, S. A. Shawkat, A. N, and, A. Farouk, “Secure Medical Data Transmission Model for IOT - Based Healthcare Systems,” IEEE Access, vol. 6, pp. 20596-20608, 2018.

[45]. N. Taeyoung, and, K. Munchurl, “A Novel No-Reference PSNR Estimation Method with Regard to Deblocking Filtering Effect in H.264/AVC Bitstreams,” IEEE Transactions on Circuits and Systems for Video Technology, vol. 24, no. 2, pp. 320-330, 2014.)