An Improved GIFT Lightweight Encryption Algorithm to Protect Medical Data In IoT

Aymen Mudheher Badr, Lamia Chaari Fourati, Samiha Ayed

An Improved GIFT Lightweight Encryption Algorithm to Protect Medical Data In IoT

1st Aymen Mudheher Badr
Digital Research Center of Sfax (CRNS)
Laboratory of Signals, Systems,
Artificial Intelligence and Networks
(SM@RTS)
Sfax University
IRAQ
aymen.m.badr@uodiyala.edu.iq

2nd Lamia CHAARI FOURATI
Digital Research Center of Sfax (CRNS)
Laboratory of Signals, Systems,
Artificial Intelligence and Networks
(SM@RTS)
Sfax University
TUNISIA
lamiachaari1@gmail.com

3rd Samiha AYED
Institute Charles Delaunay-ERA
University of Technology of Troyes
France
samiha.ayed@utt.fr

***Abstract*—The Internet of Things (IoT) enables the interconnection of devices that collect massive amounts of data, making IoT security requirements crucial and secured through encryption. However, traditional encryption protocols are no longer suitable for all IoT scenarios. We propose a new lightweight encryption method optimized for patient information protection in healthcare, considering the limited capacity of portable medical devices. Our method has been experimentally demonstrated to be effective, with a largest entropy of 7.9917 in medical images (computed tomography) and average coding and decoding times of 3.8952 sec and 3.0584 sec, respectively. The encoded image exhibits an even distribution of pixels and lower correlation coefficients between neighboring pixels, supporting the effectiveness of our less complex method compared to current state-of-the-art methods.**

***Index Terms*—IoT, Chaotic, Security, GIFT, IoMT**

I. Introduction

For Internet of Things (IoT) devices that are limited in storage space, processing speed, or battery life, a specialized field of cryptography known as lightweight encryption has been developed. Many commonly used encryption methods are vulnerable to attack. Lightweight Encryption Algorithm (LEA) is just one of many such algorithms available, including several others with varying degrees of complexity. Consequently, there is a rising need to develop and implement lightweight encryption algorithms to solve the challenge of applying encryption methods to resource-restricted devices on the Internet of Things setting. Using an encryption key or keys, cryptography is the practice of making data or messages unreadable to the naked eye [1]. Over time, several different encryption algorithms have been developed, each with its own set of pros and cons. These algorithms are time-consuming to implement, energy-intensive, and resource-intensive. A newer technique dubbed a "lightweight" encryption system has been introduced due to the need for a different approach to encryption for low-powered devices (such as portable medical equipment and IoT gadgets) [2].

Substitution permutation networks (SPNs), represented by the structure of repeated product zeros, were proposed by Feistel in 1975 and are among the most well-known and ancient scientific mathematical sequences used in the cypher area for blocks. S-boxes, also known as substitution permutation networks, are used to link together a sequence of substitution rounds [3]. The GIFT cryptographic system, which combines a block cipher algorithm with a substitution permutations network example, is one of the simplest (and most effective) [4]. The GIFT algorithm's implementation mechanism consumes little resources and produces accurate results while being extremely lightweight and memory-efficient. Since the algorithm's (Add Round Key) feature exploits the algorithm's weak key mechanism, it is vulnerable to information leakage [5].

In encryption, a "key" is a piece of data used to encrypt and decrypt files. It can be a string of numbers or letters that, when run through an algorithm, reveals the encrypted or decrypted data. The strength of encryption depends on the size and nature of the key used. It's essential to keep the key secret to maintain encryption integrity. Several factors, such as algorithm, key size, generation, and exchange, contribute to overall security. Randomly generated keys with enough entropy to avoid guessing are necessary [6]. Random key generation is a complex issue and has been addressed in various ways by cryptographic systems [7].

The output of a machine called a Random Bit Generator (RBG) can be used to produce a key directly. RBGs produce a sequence of bits that are completely random and unbiased. To create an asymmetric key pair, RBG can be used to generate either a symmetric key or random data. Alternatively, a key can be produced indirectly from another key or a password during a key agreement process [8].

Mathematical methods in chaotic cryptography use chaos theory to securely transmit information between parties or adversaries. Despite interest in this approach since 1989, concerns around security and speed have slowed its deployment [9]. A chaotic cipher consists of two halves: the cipher itself and the analysis of the cipher. Cryptanalysis involves deciphering encrypted messages, while cryptography involves encoding information for secure transmission [12]. Effective implementation of chaos theory in coding requires chaotic maps, which use the map's entropy to generate necessary noise and propagation. This research proposes a hybrid method to

generate cryptographic keys, using a pseudo-random number generator based on a chaotic system type (Lozen's approach) or Chaos Theory, to improve the performance of the GIFT algorithm [11].

Encryption is a crucial data protection method used in healthcare to safeguard electronic health records (EHR) and personal health information (PHI) against malicious intent and privacy breaches. Portable medical devices used to transmit patient data over the Internet of Things require protective techniques that do not drain power reserves. This work proposes a lightweight encryption algorithm to protect medical files and implements blockchain to authenticate data authenticity during storage. The proposed algorithm produced favorable results when compared to older encryption methods.

The following is the outline that this paper will adhere to: references to related literature are provided in Section II. In this section, the suggested methodology is broken down into its most fundamental components and laid forth for consideration in Section III. Section V provides a thorough explanation of the proposed systems used in Section IV. Metrics of performance are explained in Section V. The proposed system's effectiveness is evaluated and explained in Section VI. The concluding findings of the study are presented in Section VII of the article.

II. RELATED WORKS

In this section, the significant literature that has been published in recent times will be discussed. The researchers begin with a summary of prior work in this area and a discussion of its main shortcomings when it comes to protecting the confidentiality of patient's medical records. The proposed approach is briefly described at the end of this section. Privacy of patients' medical information is important because it is becoming a valued commodity. Compression, Authentication, Hybrid, and Encryption are just a few of the cryptographic techniques presented to ensure the safety of videos and digital images. Encryption strategies based on the most recent findings have been recommended to protect users' personal information [13], [15].

For instance, Wei et al. [16] A new encryption cryptosystem has been developed for multimedia social networks, using transformation techniques like the Latin square, chaotic maps, neural networks, and DNA technique encryption. Chaotic maps encryption is particularly efficient and widely used in contemporary cryptography. The system allows approved users to obscure unwanted human faces by restricting blurring capabilities.

Nonlinear dynamics are presented in two forms in the literature: discrete systems, like a logistic map, and continuous systems, like a hyper-chaotic system [17]. These systems' primary cryptographic utility is their ability to produce random number sequences with high-quality stochastic behavior. Recently, Hamza et al. [18] presented a Zaslavsky chaotic map-based encryption cryptosystem for digital image security. Without any finite-precision computing, the resultant chaotic signals were employed immediately in the permutation stage.

Furthermore, the starting values of the chaotic maps are quite sensitive to change. As a result, these seed values served as the private keys in chaos-based encryption systems developed by cryptographers. Pseudo-random number generator (PRNG) algorithms based on chaotic systems are well-known examples of such cryptographic applications. The commonly-employed pseudo-random number generator for chaotic-encryption-scheme stream-key generation. To encrypt images and other data, one example is Hu et al.

[19] the presentation of a pseudo-random number generator (PRNG) based on a high-dimensional chaotic map, which makes use of the combination of three coordinates of the chaotic orbits.

Furthermore, Hamza et al. [20] suggest a patient-privacy-protecting chaos-based encryption cryptosystem. The suggested cryptosystem protects patient photos from hacked brokers. For the purpose of prioritizing and securing medical keyframes extracted during a wireless capsule endoscopy surgery, we present a rapid probabilistic cryptosystem. Our cryptosystem's encrypted images are random, ensuring computational efficiency and keyframe security against multiple assaults. Additionally, it decrypts medical data only for authorized users to protect patient privacy [21].

Hasan et al. [22] provides a fast, lightweight encryption algorithm for healthcare image encryption. The lightweight encryption method secures medical images using two permutation methods. Security and execution time are compared to normally encrypted methods. The algorithm was tested on many photos. Masood et al. [23] provide a fast, lightweight encryption algorithm for healthcare image encryption. The lightweight encryption method secures medical images using two permutation methods. Security and execution time are compared to normally encrypted methods. Numerous test photos have been utilized to evaluate the proposed technique.

III. THEORETICAL BACKGROUND

A. Internet of Medical Things

New technology and energy sources are introduced every day, including the latest 1G to 5G [24] networks used in IoT applications and systems. However, high bandwidth and frequency may pose privacy and security concerns, requiring proper protocols and policies to address them. Medical devices and systems, such as consumer health monitors and pacemakers, communicate wirelessly via Bluetooth or proprietary protocols, transmitting vital data to doctors and patients. However, legacy medical devices and techniques still in use may not support modern Endpoint Detection and Response (EDR) systems, leading to security and privacy concerns. To address these issues, three factors must be considered for IoMT-enabled security: identifying networked devices, enforcing communication protocols, and checking for tampering with internal systems. Encryption is a useful tool for safeguarding diagnostic images in IoMT applications, where unauthorized image copying or usage may occur [25].

B. GIFT Block Cipher

The GIFT block cipher uses symmetric key cryptography with the Substitution Permutation Network (SPN) method. Both GIFT-64/128 (a 64-bit block with a 128-bit key) and GIFT-128/128 are viable choices (128-bit block and 128-bit key). The four operations of Sbox, Permutation, AddRoundKey, and Constant XOR are performed in each round of the GIFT block cipher. Figure 1 depicts the encipherment procedure of the GIFT block cipher [26].

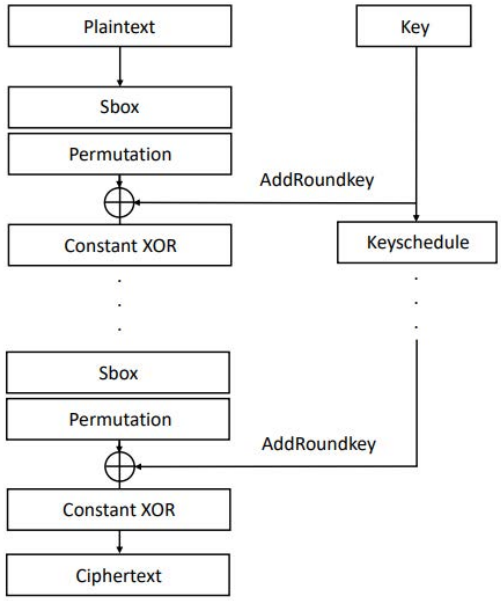

Fig. 1. Encryption process of GIFT block cipher.

1) GIFT Block Cipher Sbox: The 4-bit Sbox's input value is the n-bit block (n = 64, 128) after it has been divided into 4 bits. Table 1 provides the GIFT block cipher's Sbox [20].

TABLE I
SBOX OF GIFT BLOCK CIPHER

x	0 1 2 3 4 5 6 7 8 9 a b c d e f
Sbox(x)	1 a 4 c 6 f 3 9 2 d b 7 5 0 8 e

2) GIFT Block Cipher Permutation: The GIFT-64/128 permutation swaps out the P64 i-th bit of block B with the i-th bit of block B. Table 2 provides information on the permutation of GIFT-64/128. This document omits the full Table on GIFT-128/128 permutation [20].

3) GIFT Block Cipher's AddRoundkey: k0 and *k1* (a combined 32-bit value) are chosen from the key (K =*k7,..., k0*) in the GIFT-64/128 block cipher. In the round key, *k0* and *k1* are utilized as U and V, respectively. RK = U$\|$V =*u*15...*u*0$\|$*v*15...*v0* (U = *k1*, V = *k0*). The round key is XORed to *b4i+1*, and V to *b4i* to form an exclusive-ore with the block B.

$$b_{4i+}1 \leftarrow b_{4i+}1 \oplus u_i, b_{4i} \leftarrow b_{4i} \oplus v_i, i = 0, ..., 15 \quad (1)$$

TABLE II
GIFT-64 BIT PERMUTATION

i	0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15
$P_{64}(i)$	0 17 34 51 48 1 18 35 23 49 2 19 16 33 50 3
i	16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
$P_{64}(i)$	4 21 38 55 52 5 22 39 36 53 6 23 20 37 54 7
i	32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47
$P_{64}(i)$	8 25 42 59 56 9 26 43 40 57 10 27 24 41 58 11
i	48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63
$P_{64}(i)$	12 29 46 63 60 13 30 47 44 61 14 31 28 45 62 15

In the GIFT-128/128 block cipher, k0, k1, k4, and k5 (64-bit in a total) are selected from the key K. k0, k1, k4 and k5 are used as U and V of the round key as follows, RK = U$\|$V = u31...u0$\|$v31...v0 (U = k5$\|$k4, V = k1$\|$k0). The round key is XORed to the block B, where U is XORed to b4i+2 and V is XORed to b4i+1.

$$b4i+2 \leftarrow b4i+2 \oplus ui, b4i+1 \leftarrow b4i+1 \oplus vi, i = 0, ..., 31 \quad (2)$$

4) GIFT Block Cipher Constant XOR: The GIFT-64/128 and GIFT-128/128 block ciphers employ the round constants C listed in Table 3. Block B is created by XORed single-bit and round constants (C = c5c4c3c2c1c0) together as in Equation (3).

$$b_{n1} \leftarrow bn_1 \oplus 1, b_{23} \leftarrow b_{23} \oplus c_5,$$
$$b_{19}b_19 \oplus c_4 b_{15} b_{15} \oplus c_3, b_{11} \leftarrow b_{11} \oplus c_2, b_7 7 \oplus c_1, b_3 b_3 \oplus c_0. \quad (3)$$

TABLE III
ROUND CONSTANTS C

Rounds	Constants C
1 to 16	01 03 07 0F 1F 3E 3D 3B 37 2F 1E 3C 39 33 27 0E
17 to 32	1D 3A 35 2B 16 2C 18 30 21 02 05 0B 17 2E 1C 38
33 to 48	31 23 06 0D 1B 36 2D 1A 34 29 12 24 08 11 22 04

5) GIFT Block Cipher Keyschedule: The Key schedule in GIFT-64/128 and GIFT-128/128 block ciphers updates the key (K = k7,..., k0) and extracts the round key from the updated key K. Equation (4) depicts the Key schedule. The symbol (i) represents a right rotation operation (i-bit) [20].

$$k_7 \| k_6 \| ... \| k_1 \| k_0 \leftarrow k_1 \rangle\rangle 2 \| k_0 12 \| ... \| k_3 \| k_2, \quad (4)$$

C. Chaotic Chen System

Chaos theory is a mathematical and scientific study of highly sensitive dynamical systems that were previously thought to be completely chaotic and irregular. Even seemingly chaotic and complex systems exhibit underlying patterns, repetition, self-similarity, fractals, and self-organization to those knowledgeable in chaos theory. The butterfly effect as of Figure (2), a central notion of chaos theory, describes how a small perturbation in one state of a nonlinear system can have a significant impact on another state due to sensitive dependence on initial conditions. The proposed strategy utilizes the Lorenz

Attractor, which demonstrates how data changes over time and shows that it is almost impossible to know all the infinite numbers of data [23].

Edward Lorenz's 1963 atmosphere model simplification was a significant step forward in understanding atmospheric change, as it simplified the process to a differential equation in Eq.5.:

$$\frac{dx}{dt} = \alpha(y - x) \tag{5}$$

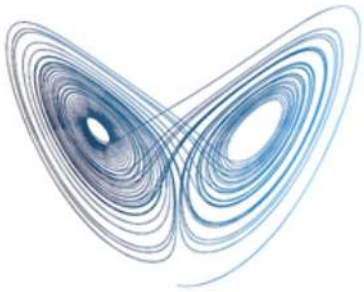

Fig. 2. Lorenz attractor

$$\frac{dy}{dt} = x(\beta - z) \tag{6}$$

$$\frac{dz}{dt} = xy - \gamma z \tag{7}$$

Where: Alpha is a Prandtl number, Beta is proportional to the Rayleigh number Gamma is a geometric factor.

IV. THE PROPOSED SYSTEM

This innovative way to generate random keys for chaotic systems is called Chaos Theory, and it is the basis for the suggested method (CSKey) (Lozens method). The CSKey produces a string of completely random digits. Using these random numbers and a lightweight GIFT algorithm, CSKey performance was enhanced and a robust chaotic encryption mechanism was made available for Internet-of-Things (IoT) equipment transmitting medical data. It is demonstrated in Figure (3) and Figure (4) that the suggested technique uses the initial values for these maps.

V. THE METRICS OF PERFORMANCE

Performance quality is a cornerstone criterion for assessing lightweight encryption methods. Here, we'll detail our research into the GIFT algorithm's implementation and show how we tested it, both with and without the proposed Chaos Secret Key (CSKey). We will evaluate the effectiveness of the proposed key in the algorithm by comparing it to the standard approach. Performance metrics refer to a wide variety of indicators that have widespread worldwide recognition [24],[25].

- Entropy, High-entropy images are more secure as they contain more randomness, making decryption without the key difficult. Low-entropy images have less randomness and are more vulnerable to attacks.

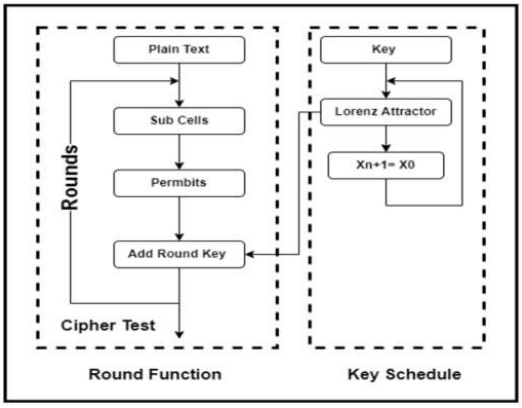

Fig. 3. Original Encryption algorithm (Gift)

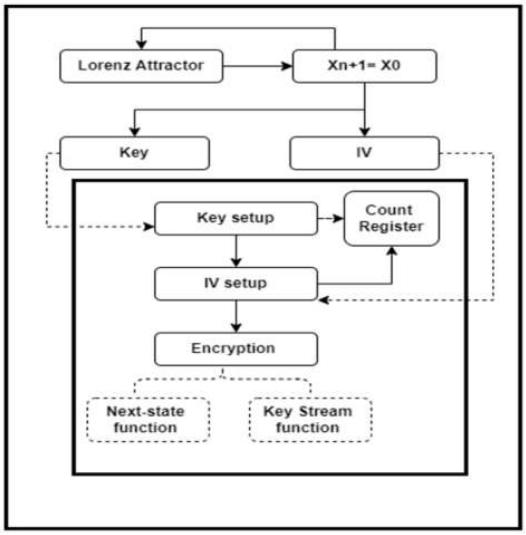

Fig. 4. Modify Encryption algorithm (Gift)

$$H = -p(i) * log2(p(i)) \tag{8}$$

where: H is the entropy of the system, p(i) is the probability of the i-th possible outcome of the system, and log2 is the base-2 logarithm.

- Mean squared error (MSE) is the most widely used estimate statistic for image quality. as seen in Eq.(8).

$$MSE = \frac{1}{n}\sum_{i=1}^{n}[I(i) - k(i)]^2 \tag{9}$$

- Peak Signal-to-Noise Ratio (PSNR) measures signal representation quality relative to noise distortion in Eq.(9). It includes both extreme and intermediate values for quality assessment.

$$PSNR = 20.\log_{10}(MAX_i) - 10.\log_{10}(MSE) \tag{10}$$

where: MAXi is the maximum possible pixel value of the image.

- Measurement of the Universal Quality Image Index(UQI): measures image quality after modifications, is easy to compute, and can be applied to various image processing programs. [23].

$$UQI = 1\frac{1}{M}\sum_{j=1}^{m} Qj \tag{11}$$

- Measuring the structural similarity index (SSIM), how similar a recovered image is to the original by calculating the structural similarity index based on an inferential model that perceives image degradation as a shift in structural information.

$$SSIM(x,y) = [l(x,y)]^{\alpha} * [c(x,y)]^{\beta} * [s(x,y)]^{\gamma} \tag{12}$$

- SCC measures spatial correlation and is similar to measuring the intensity of a linear relationship between x and y, where the average gain of the incoming signal correlates with its angle of arrival.

$$SCC = \frac{[\sum\sum(I(x,y) - \mu I) * (K(x,y) - \mu K)]}{[\sigma I * \sigma K]} \tag{13}$$

- Number of Changing Pixels Rate (NPCR) is the rate at which the cipher picture's pixel count shifts in response to a shift of a single pixel in the plain image.

$$NPCR = \frac{Nc}{N} * 100\% \tag{14}$$

where: Nc is the number of pixels that change between the two encrypted images, and N is the total number of pixels in the images.

- Unified Average Changing Intensity (UACI) is used to determine the level of dissimilarity between a plain image and a ciphered image.

$$UACI = (1/n) * \frac{\sum\sum|I(x,y) - K(x,y)|}{MAXi} \tag{15}$$

where: I(x, y) and K(x, y) are the intensities of the two images at the pixel location (x, y), n is the total number of pixels in the images, and MAXi is the maximum possible pixel value of the image (e.g., 255 for an 8-bit grayscale image).

VI. RESULT AND DISCUSSION

The researchers have conducted a variety of experiments to measure the robustness and reliability of the suggested cryptosystem. Experiments and measurements are taken to ensure the system is secure against several types of attacks, such as statistical, secret-key, and differential ones as shown in Table (4) and (5), and Table (6) and (7) shone the values of correlation.To begin, a histogram analysis is presented to show that the encrypted images' pixels are distributed uniformly and in a way that is fundamentally different from the histograms of the plain images. The next step is to calculate the image's information entropy, which proves the image's randomness and its resistance to entropy attacks. The correlation coefficient demonstrates that the suggested cryptosystem reduces the correlation between neighboring pixels of the plain image sequentially. Differential attacks are evaluated with the help of the number of pixels changing per second (NPCR) and the unified average changing intensity (UACI) tests. The power of our cryptosystem to withstand extensive attacks is uncovered through analysis of the secret keys. The probabilistic analysis carried out here demonstrates that the same keyframe and the same secret keys result in radically distinct encrypted keyframes produced by the cryptosystem. In addition, the sensitivity analysis proves beyond a reasonable doubt that recovering the original frames from the backup requires knowing the precise values of the secret keys. Thus, the encrypted image will change drastically if the secret keys are ever changed. Image quality analysis further substantiates the excellent state of the encrypted image. To ensure that a cryptosystem is secure, anti-clipping analysis simulates scenarios in which some pixels from some blocks are clipped off. In the end, the comparative study proves that our cryptosystem is far superior to the current state of the art.

Histograms plot the number of pixels at each level of color intensity, providing a visual representation of the image's pixel distribution. The goal of this check is to ensure that the histogram and distribution of pixel values in the encrypted image are different from the original. The original, encrypted, and decrypted photographs are all displayed in Figure (5). Histograms of the keyframes and encrypted images for each of the three RGB components are displayed in Figure (6). Histograms of the three encrypted images are consistent and dissimilar to those of the keyframes. The suggested cryptosystem's efficacy in removing correlation between neighboring pixels of a keyframe is demonstrated by the correlation coefficient test. When two random variables are correlated, it shows how strongly and in what direction they are related along a linear axis. This allows for analyzing the relationship between neighboring pixels in both the encrypted and unencrypted versions of the keyframe. Given the vast number of possible pixel combinations in a medical keyframe, randomly select 1024 pairs of adjacent pixels to examine for correlation in the x, y, and z axes, as shown in Figure (7).

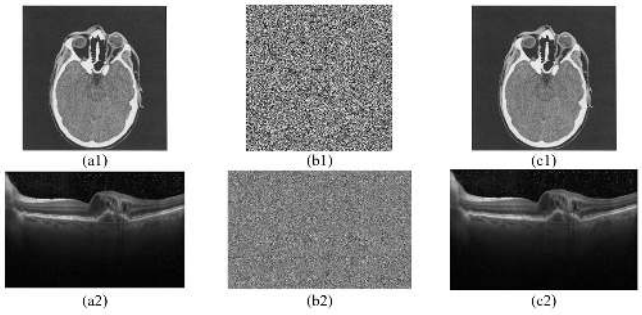

Fig. 5. Photographic encryption tests (a) Original Images (b) Encrypted Images and (c) Decrypted Images

TABLE IV
PERFORMANCE WITH ORIGINAL GIFT (IMAGE SIZE 256*256)

Images	UACI	NoCPR	MSE	PSNR	Universal Quality	SSIM	SCC	Entropy
Lena	21.9514	99.4766	8955.3149	8.6099	0.7044	0.0179	0.0040	7.7515
Baboon	19.9198	99.4171	8241.2747	8.9708	0.7355	0.0189	-0.0004	7.6980
Pepper	23.2789	99.4568	10059.9406	8.1048	0.6031	0.017228	0.00028	7.7338
Car	24.4880	99.5056	9106.0540	8.5375	0.7485	0.01935	0.0014	7.5102
CTimage1	31.3814	99.5926	9531.6585	8.3391	0.5855	0.00749	0.0010	6.3374
CTimage2	31.4622	99.6293	15282.2397	6.2889	0.2223	0.010129	0.00063	6.5862

TABLE V
PERFORMANCE WITH MODIFIED GIFT (IMAGE SIZE 256*256)

Images	UACI	NoCPR	MSE	PSNR	Universal Quality	SSIM	SCC	Entropy
Lena	21.9240	99.4751	8949.4747	8.6128	0.7043	0.0204	0.0008	7.9989
Baboon	19.9766	99.4141	8252.2265	8.9650	0.7353	0.0199	-0.0013	7.9991
Pepper	23.3229	99.5117	10069.8229	8.1005	0.6025	0.0186	0.0010	7.9990
Car	24.5377	99.4873	9174.9437	8.5047	0.7468	0.0203	-0.0010	7.9997
CTimage1	31.2235	99.6231	9459.2237	8.3722	0.5874	0.0120	-0.0316	7.9917
CTimage2	31.4529	99.6039	15300.5571	6.2837	0.2219	0.0112	0.004206	7.9920

TABLE VI
CORRELATION COEFFICIENTS BETWEEN ADJACENT PIXELS TO ORIGINAL GIF

Correlation Horizontal	Correlation Vertical	Correlation Diagonal
-0.0054	0.01807	0.0498
0.0112	-0.0144	0.0023
0.0324	-0.0171	-0.0024
0.0135	0.0305	0.0057
-0.0193	-0.0059	-0.0101
-0.0155	0.0024	-0.0081

TABLE VII
CORRELATION COEFFICIENTS BETWEEN ADJACENT PIXELS TO MODIFIED GIF

Correlation Horizontal	Correlation Vertical	Correlation Diagonal
-0.0047	0.0012	0.0204
0.0016	0.0168	-0.0234
-0.0074	-0.0057	0.0096
0.0731	0.0183	-0.0016
-0.0122	-0.0231	0.0020
0.0117	-0.0075	-0.0206

The comparative test is an important demonstration of the proposed cryptosystem's overall efficiency in relation to other state-of-the-art cryptosystems, particularly in ensuring rising suitability for real-world applications. As was demonstrated in the preceding subsections, we carried out a variety of comparison experiments. The findings revealed that our cryptosystem possesses superior performance when measured against other published studies [14] – [17], [19], [23]. Here, the results show how the proposed cryptosystem stacks up against other cutting-edge encryption solutions by conducting more extensive comparison tests based on a variety of experimental analyses. According to Table (6), the suggested cryptosystem is just as effective as competing systems when measured against a variety of analysis metrics (NPCR and UACI). Taking into account these advantages, the suggested cryptosystem can ensure patients' confidentiality and safety.

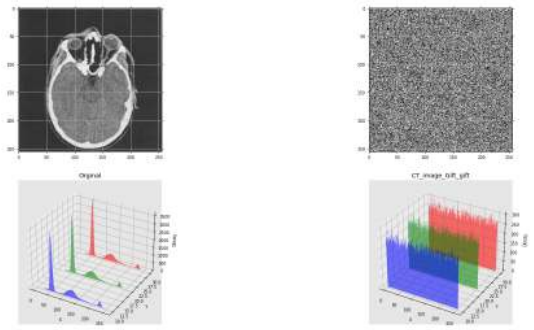

Fig. 6. The histogram test of the Original Image and encrypted image with GIFT in the three Red, Green, and Blue components

TABLE VIII
ANALYSES BASED ON A NUMBER OF DIFFERENT METRIC COMPARISONS

Method	Image size	NPCR analysis	UACI analysis	Sensitivity analysis
Proposed	[256,256,3]	99.6231	31.2235	Yes
[23]	[640,480,3]	99.609	33.465	Yes
[16]	[1024,1024,1]	99.617	33.669	Yes
[19]	[256,256,1]	99.61	33.50	Yes
[17]	[256,256,3]	99.217	33.405	Yes
[14]	[640,480,3]	99619	33.477	Yes
[15]	[640,480,3]	99.606	44.486	Yes

VII. CONCLUSION AND FUTURE WORK

This paper suggested a fast and reliable picture cryptosystem to keep medical records private. During its transfer to

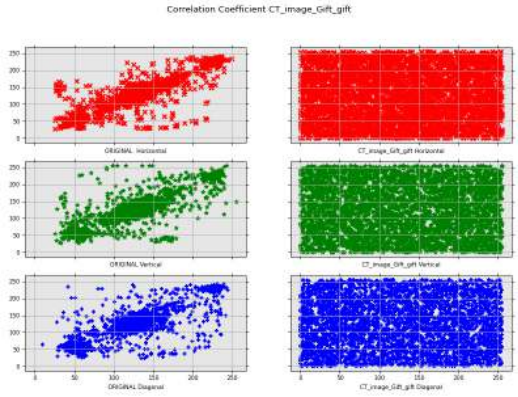

Fig. 7. Before encryption, horizontal, vertical, and diagonal correlation of two neighboring pixels in the three spectral components (R, G, and B)

hospitals and clinics, sensitive medical data is protected by the suggested cryptosystem. This cryptosystem makes use of a variant of the GIFT algorithm that makes use of two different types of chaotic maps. The encryption keys for the proposed improved GIFT are generated by combining and cascading the orbits of two of the 2D chaotic maps. In this proposed cryptosystem, a block symmetric encryption technique was used, constructed from a single round of confusion and diffusion. According to the study, the present approaches provide key-based, non-systematic sequence numbers that require lengthy computations. Comparatively, it is clear from the outcome that the computation required by the suggested algorithm is little. As a result, the suggested algorithm is carefully constructed to obtain the highest level of security in order to secure the medical image. The image is encrypted using three steps of encryption using a 256-bit key value for logical operation. The suggested cryptosystem also utilized the keyframe boundary to secretly incorporate noise (random) values that would not be discernible in the decoded image. The performance of our cryptosystem is exceptional, and it is able to effectively withstand a wide variety of assaults, including differential, statistical, and exhaustive attacks for the purpose of discovering secret keys. Extensive experimental findings and security analysis showed that the suggested cryptosystem is both quicker and safer than existing methods. When using the proposed cryptosystem, sensitive medical data contained in keyframes is protected. In addition to protecting patients' confidentiality, this method also saves time, money, and resources by decreasing the need for power, communication, analysis, and searching. To further increase the effectiveness of the proposed cryptosystem and to open new directions in this field of research, the researcher plans to investigate access control mechanisms and homomorphic encryption algorithms in the future.

REFERENCES

[1] Kubba, Zaid M. Jawad, and Haider K. Hoomod. "Developing a lightweight cryptographic algorithm based on DNA computing." AIP Conference Proceedings. Vol. 2290. No. 1. AIP Publishing LLC, 2020.

[2] Shetty, Vaishnavi S., et al. "A survey on performance analysis of block cipher algorithms." 2020 International Conference on Inventive Computation Technologies (ICICT). IEEE, 2020.

[3] Sehrawat, Deepti, and Nasib Singh Gill. "Lightweight block ciphers for IoT based applications: a review." International Journal of Applied Engineering Research 13.5 (2018): 2258-2270.

[4] Heys, Howard M. "A Tutorial on the Implementation of Block Ciphers: Software and Hardware Applications." Cryptology ePrint Archive, 2020.

[5] Cohney, Shaanan, et al. "Pseudorandom black swans: Cache attacks on CTR-DRBG." 2020 IEEE Symposium on Security and Privacy (SP). IEEE, 2020.

[6] Mousavi, Seyyed Keyvan, et al. "Security of internet of things based on cryptographic algorithms: a survey." Wireless Networks 27.2 (2021): 1515-1555.

[7] Salau, Ayodeji Olalekan, Nikhil Marriwala, and Muzhgan Athaee. "Data security in wireless sensor networks: attacks and countermeasures." Mobile radio communications and 5G networks. Springer, Singapore, 2021. 173-186.

[8] Dasgupta, Dipankar, John M. Shrein, and Kishor Datta Gupta. "A survey of blockchain from security perspective." Journal of Banking and Financial Technology 3.1 (2019): 1-17.

[9] Pandey, Prateek, and Ratnesh Litoriya. "Implementing healthcare services on a large scale: challenges and remedies based on blockchain technology." Health Policy and Technology 9.1 (2020): 69-78.

[10] Moin, Sana, et al. "Securing IoTs in distributed blockchain: Analysis, requirements and open issues." Future Generation Computer Systems 100 (2019): 325-343.

[11] Lee, Tian-Fu, I-Pin Chang, and Ting-Shun Kung. "Blockchain-based healthcare information preservation using extended chaotic maps for HIPAA privacy/security regulations." Applied Sciences 11.22 (2021).

[12] Anwar, Shamama, and Solleti Meghana. "A pixel permutation based image encryption technique using chaotic map." Multimedia tools and applications 78.19 (2019): 27569-27590.

[13] Y. Wu , G. Yang , H. Jin , J.P. Noonan , Image encryption using the two-dimensional logistic chaotic map, J. Electron Imaging 21 (1) (2012).

[14] Y. Zhou , Z. Hua , C.-M. Pun , C.P. Chen , Cascade chaotic system with applications, IEEE Trans. Cybern. 45 (9) (2015) 2001–2012 .

[15] A . Belazi , A .A .A . El-Latif , S. Belghith , A novel image encryption scheme based on substitution-permutation network and chaos, Signal Process. 128 (2016) 155–170.

[16] Z. Wei, Y. Wu, Y. Yang, Z. Yan, Q. Pei, Y. Xie, J. Weng, Autoprivacy: automatic privacy protection and tagging suggestion for mobile social photo, Comput. Secur. (2018), doi: 10.1016/j.cose.2017.12.002.

[17] Z. Wei, Z. Yan, Y. Wu, R.H. Deng , Trustworthy authentication on scalable surveillance video with background model support, ACM Trans. Multimed. Comput. Commun. Appl. (TOMM) 12 (4s) (2016) 64.

[18] R. Hamza, A novel pseudo random sequence generator for image-cryptographic applications., J. Inf. Secur. Appl. 35 (2017) 119–127.

[19] Hu, L. Liu, N. Ding, Pseudorandom sequence generator based on the chen chaotic system, Comput. Phys. Commun. 184 (3) (2013) 765–768.

[20] R. Hamza , F. Titouna, A novel sensitive image encryption algorithm based on the Zaslavsky chaotic map, Inf. Secur. J.: Glob. Perspect. 25 (4-6) (2016) 162–179.

[21] R. Hamza, Z. Yan and K. Muhammad et al., A privacy-preserving cryptosystem for IoT Ehealthcare,InformationSciences,

[22] Hasan, M. K., Islam, S., Sulaiman, R., Khan, S., Hashim, A. H. A., Habib, S., Hassan, M. A.." Lightweight Encryption Technique to Enhance Medical Image Security on Internet of Medical Things Applications." IEEE Access, (2021), 9, 47731–47742.

[23] Masood, F., Driss, M., Boulila, W., Ahmad, J., Rehman, S. U., Jan, S. U., ... Buchanan, W. J. "A Lightweight Chaos-Based Medical Image Encryption Scheme Using Random Shuffling and XOR Operations. Wireless Personal Communications." (2021).

[24] FADHIL, Heba Mohammed; DAWOOD, Zinah Osamah. Evolutionary perspective of mobile communication technologies. In: 2018 International Conference on Computer and Applications (ICCA). IEEE, 2018. p. 80-84.

[25] ROUGAII, Fatima; MAZRI, Tomader. SECURE MEDICAL IMAGE ENCRYPTION FOR REMOTE VIRTUAL DOCTOR SYSTEM BASED ON H-IOT APPLICATIONS OVER 5G NETWORK: A COMPARISON STUDY. International Archives of the Photogrammetry, Remote Sensing Spatial Information Sciences, 2021, 46.

[26] Jang, Kyoungbae, et al. "Grover on GIFT." Cryptology ePrint Archive (2020).