Protecting Medical Data on the Internet of Things with an Integrated Chaotic-GIFT Lightweight Encryption Algorithm

Heba Mohammed Fadhil*1, Mohamed Elhoseny2, Baydaa M Mushgil1
1Department of Information and Communication, Al-Khwarizmi College of Engineering, University of Baghdad, Iraq
2University of Sharjah, UAE, Dubai, United Arab Emirates
Emails: heba@kecbu.uobaghdad.edu.iq ; melhosenyy@ieee.org; baydaa@kecbu.uobaghdad.edu.iq

Abstract

The preservation of medical data integrity during the transmission process is of great significance in upholding patient confidentiality and privacy. The incorporation of Internet of Things (IoT) technology in the healthcare sector has added a novel aspect, whereby the transmission of medical data across networks becomes susceptible to cyber-attacks. The statement underscores the urgent need for encryption techniques that include both lightweight and strong characteristics and effectively safeguard medical data during transmission. This paper introduces a novel amalgamation technique called "Integrated Chaotic-GIFT," which aims to achieve safe and efficient encryption of medical data conveyed over IoT networks. The proposed model utilizes ideas derived from the chaos theory in combination with a streamlined block cipher, resulting in a powerful but resource-efficient encryption method for medical data. This technique utilizes complex bit-level permutations and substitutions to encode medical pictures. Furthermore, proposed the utilization of the Chaotic-GIFT algorithm to address the safe transmission of medical data across Internet of Things networks. The Chaotic-GIFT algorithm is characterized by its lightweight nature and high efficiency, making it a suitable option for this purpose. The efficacy of the method is thoroughly evaluated by a comprehensive analysis of several metrics, including the time of encryption and decryption processes, data throughput, impact of avalanche effects, investigation of nonlinearity, and examination of correlation coefficients.

Keywords: Internet of Things, Lightweight Cryptography, Security, GIFT, Medical Information.

1. Introduction

Lightweight encryption is a subfield of cryptography tailored to the needs of Internet of Things (IoT) devices with constrained resources, such as memory, computing power, or battery life. Many popular forms of encryption can be broken [1]. There are a variety of encryption methods available that are more complex than the Lightweight Encryption Algorithm (LEA) [2]. Because of this difficulty, there is a growing interest in designing and deploying lightweight encryption algorithms for use in the IoT[3]. Cryptography is the process of rendering data or messages unintelligible to the naked eye using an encryption key or a key. Numerous encryption algorithms have been developed, each with its own advantages and disadvantages[4]. It takes considerable time, effort, and materials to develop these algorithms. Because of the necessity for a new method of encryption on low-powered devices (such as portable medical equipment and IoT gadgets), a "lightweight" encryption system has been developed [5]. Some of the oldest and most well-known scientific mathematical sequences employed in the cypher domain for blocks are substitution permutation networks.
(SPNs), which are represented by the structure of repeated product zeros and were proposed by Feistel in 1975 [6]. S-boxes or substitution permutation networks, connect successive substitution rounds. For example, one of the simplest (and most effective) cryptographic systems is the GIFT system, which combines a block cipher algorithm with an example of a substitution permutation network. The technique for implementing the GIFT algorithm has low resource requirements, is memory efficient, and yields precise results[7]. The algorithm is susceptible to information leaking because the (Add Round Key) feature takes advantage of the weak key mechanism of the program.

A "key" is a distinct data item used for encryption purposes. The data in a file can be encrypted or decrypted using a series of numbers or letters, and a suitable algorithm. It can encrypt and decode data, in an asymmetric cipher, where only encryption is feasible, or in a symmetric cipher, where both encryption and decryption are possible. The effectiveness of an encryption technique may depend on the size and composition of the key employed; however, in all cases, it is crucial that the key be kept secret to guarantee the integrity of the encryption [8]. The safety of a key depends on several factors. These include the algorithm used, size of the key, method used to generate the key, and method used to exchange keys. Keys must be produced randomly with enough entropy to prevent guessing. Different cryptographic systems have adopted different approaches to the difficult problem of secure random key creation [9]. A key can be generated directly from the output of a device known as a Random Bit Generator (RBG). The bits generated by the RBGs are fully random and impartial. A symmetric key or random data can be generated using the RBG to create an asymmetric key pair. Another option is to generate a key in a backdoor fashion via a key agreement process, using an existing key or password as inputs [10].

Mathematical techniques in chaotic cryptography use chaos theory to send information to a third party or adversary in a way that is both private and secure. Since Robert Matthews first investigated the possibility of using chaos for encryption in 1989, there has been widespread interest in doing so. However, long-standing concerns regarding security and speed have hindered their deployment [11]. A chaotic cipher consists of two parts: a cipher and its analysis. In contrast to cryptography, which encrypts data for secure transmission, cryptanalysis decodes the encrypted messages. Chaotic maps, which take advantage of the entropy of the map to generate the necessary noise and propagation, are essential for the successful implementation of the chaos theory in computer programming. This study proposes a hybrid approach for generating cryptographic keys. The GIFT algorithm uses a chaotic system (Lozen's method) or Chaos Theory-based PRNG to boost its performance [12].

The healthcare sector is increasingly using encryption to protect sensitive data. Data, in this case electronic health records (EHR), are encrypted so that only authorized parties can access them [13]. Medical records, patient histories, and other sensitive health information must be kept secure to prevent misuse or privacy breaches, which could lead to severe penalties [14]. Low-power portable medical devices are used to transmit a patient's condition to healthcare systems over the Internet of Things; therefore, there is a need to focus on protective strategies that do not drain the devices' limited battery reserves. Because we will be dealing with portable medical equipment connected to the Internet of Things, this work proposes an approach for protecting medical files by developing a lightweight encryption algorithm, which has shown promising results when compared to previous ones [15].

The structure of this paper is as follows: Section II includes a bibliography of relevant works. The proposed methodology is deconstructed into its components and is discussed in Section III. Section IV elaborates on the implemented systems. Performance measures are broken down in Section V. The evaluation and clarification of the efficacy of the proposed system are presented in Section VI. The results of this study are presented in Section VII.

2. Related Works
The latest significant literature review covers previous research on this subject. Its noted ineffectiveness in protecting patients' medical records. The proposed technique is briefly described in the conclusion section. Protecting patients' medical data has become more important as it becomes an asset. Compression, authentication, hybrid approaches, and encryption have all been implemented to secure digital photographs.
and videos. New encryption techniques [16]– [18] have been proposed for the sake of user privacy. For authorized users on multimedia social networks, Wei et al. [19] created an encryption cryptosystem to obscure people's faces. Mathematics and transformation techniques, such as the Latin square, chaotic maps, neural networks, and DNA-based encryption, are currently the most effective cryptographic practices. Chaotic map encryption is popular in modern cryptography owing to its effectiveness. The literature on nonlinear dynamics classifies systems into two categories: continuous ones, such as hyperchaotic ones, and discrete ones, such as the logistic map. The fundamental cryptographic value of these systems lies in the generation of high-quality stochastic number sequences. Hamza et al. [20] unveiled an image-encryption method based on Zaslavsky chaotic maps. The chaotic signals of this map were integrated into the permutation stage without requiring approximate computations. The initial values of the chaotic maps are sensitive to modifications; thus, cryptographers use them to create private keys for chaos-based encryption schemes. PRNG algorithms based on chaotic systems are used in cryptography. The most popular PRNG usage for chaotic encryption is stream key generation. Hu et al. [21] used a high-dimensional chaotic map and three chaotic orbit coordinates to create a pseudo-random number generator (PRNG) for encrypting photos and other data.

An image encryption technique using quasigroups and chaotic standard maps was proposed by Patidar et al. [22] used the Shannon-based substitution-diffusion technique uses a quasigroup of order 256 and a chaotic standard map for pixel substitution and permutation. Integrating quasigroups with the chaotic standard map parameter and initial conditions greatly extends the key space. Simple quasigroup-based substitution using lookup table operations on Latin squares (Cayley operation tables of quasigroups) makes this technique more efficient. Performance and security evaluations and extensive statistical analysis (using tools such as histograms, correlation coefficients, information entropy, key sensitivity, differential analysis, and key space analysis) verified the safety of this picture cipher. Hamza et al. [23] developed a chaos-based encryption cryptosystem for patient privacy. This technology protects patients’ photographs from unwanted access. Researchers have developed a quick probabilistic cryptosystem to prioritize and encrypt medical keyframes collected during wireless capsule endoscopy procedures. The encrypted pictures were purposely randomized to maximize computational efficiency and ensure security against various attackers. This technology only decrypts medical data for authorized users, thereby protecting patient privacy.

Color image encryption (CIEA) was developed by Hua et al. [24] used a two-dimensional logistic tent modular map (2D-LTMM). The 2D-chaotic LTMM's range is larger and more continuous, and its trajectory distribution is even greater than that of any other chaotic map used for image encryption. The LTMM-CIEA method accomplishes these characteristics using cross-plane permutation and non-sequential diffusion. Non-sequential diffusion processes pixels in an obscure and random order, whereas cross-plane permutation shuffles row and column locations across all three-color planes. To circumvent the limitations imposed by chaotic maps, this study developed 2D-LTMM and LTMM-CIEA to encrypt images over-all three-color dimensions. 2D-LTMM outperforms recently created chaotic maps, and LTMM-CIEA outperforming several state-of-the-art image encryption methods based on extensive simulations and security evaluations.

Askar et al. [12] developed a logistic and two-dimensional chaotic economic map-based encryption method. The resilience of the algorithm is shown by its image-type applications. Statistical examinations of the key space sensitivity, pixel correlation, entropy processes, and contrast partially prove the security of the algorithm. The key security space, sensitivity to the secret key, minimal correlation coefficients, heightened contrast, and acceptable entropy information of the algorithm are shown in the findings and comparative studies. The robustness of the algorithm against statistical, differential, brute-force, and noise assaults were further demonstrated via experiments.

Hasan et al. [25] developed a fast, lightweight healthcare picture data encryption technique. This approach encrypts medical images using dual permutation. Extensive testing on a variety of images compares the security and execution time of the algorithm to those of existing encryption methods. Masood et al. [26] developed a fast, lightweight encryption technique for healthcare picture security. This lightweight
solution protects medical pictures using two permutations. Using a wide range of test pictures, they were compared with traditional encryption techniques for security and execution time.

This section summarizes the current research on cryptographic advances to secure healthcare data. The proposed methods handle medical pictures and data encryption issues with varying strengths.

3. Theoretical Background

This section offers a theoretical background that underlies the proposed technique for lightweight encryption of medical data in contexts that make use of the Internet of Things (IoT). It provides an overview of fundamental ideas such as encryption techniques and chaotic systems, as well as the applicability of these ideas to the task of preserving the confidentiality of data in environments with limited resources.

A. Internet of Medical Things

Every day, give introduction of a new technology, a new form of energy, or a new twist on an old method. Newer 1G to 5G networks have been utilized in IoT applications and infrastructure. Academics are interested in this area because of the possibility of breaches in privacy and security, particularly at high bandwidths and frequencies [27]. More base stations in the same area may be required for short-wavelength wireless networks. Possible dangers associated with the new design include the spread of false base stations. When deciding whether to use the Internet of Medical Things (IoMT) [25], hospitals and healthcare organizations must weigh the benefits against the need for appropriate protocols and policies to address security concerns. Nike Fuel Band, Fit Bit, and other consumer health monitors connect to mobile systems via Bluetooth to keep tabs on users' fitness and health data. Implanted medical equipment, such as pacemakers, communicate wirelessly with one another using Bluetooth or proprietary protocols. Wearable medical technologies, such as mobile insulin pumps. These gadgets send critical information to doctors and patients via proprietary wireless protocols. Stationary medical equipment includes chemotherapy systems in hospitals and heart monitoring monitors in homes. In these setups, data are transferred via Wi-Fi networks. For over 15 years, medical practitioners have relied on tried-and-true methods and equipment. X-ray machines, pulmonary function tests, and computed tomography (CT) scans are often used in hospitals and healthcare facilities. Even if these gadgets do not work with state-of-the-art Endpoint Detection and Response (EDR) systems, security and privacy worries persist [28].

IoMT-enabled security is influenced by three aspects. The first step is to locate networked gadgets. Second, it is mandatory for all connected software and hardware to interact in a certain manner. Finally, no other network devices or internal systems have been tampered with by the IoMT devices[29]. Using IoMT apps, medical professionals from around the world have easy access to enormous numbers of digital images for diagnosis, replication, data storage, and retrieval. In many cases, this leads to illegal reproduction or utilization. There has been much research on the protection of images in IoMT applications. Since this is the case, diagnostic picture encryption is a useful tool [30].

B. Chaotic Theory System

The study of dynamical systems that were originally thought to be in fully chaotic and irregular states but are now recognized to be highly sensitive to their initial circumstances, is the focus of chaos theory, which is a branch of mathematics and science. These systems operate in accordance with regularities and laws. Even seemingly chaotic and complicated systems show underlying patterns, connectivity, ongoing feedback loops, repetition, self-similarity, fractals, and self-organization to those familiar with the chaos theory [31].

In chaos theory, the butterfly effect (see Figure (1)) describes how seemingly insignificant shifts in one state of a nonlinear, deterministic system can have far-reaching consequences for a different state (i.e., there is a sensitive dependence on initial conditions). The butterfly effect is commonly represented by the idea that a butterfly wingbeat in Brazil may trigger a hurricane in Texas [32]. Considering this, even modest alterations
to complex systems can have far-reaching and unanticipated consequences. Any arbitrary pattern from the path of a meteor or asteroid to the acts of a single person could serve as the design in this case, which was extremely sensitive to even slight changes. For this reason, scientists have coined the phrase "sensitive dependence on starting conditions" to characterize it. The proposed technique uses a chaotic map known as the Lorenz Attractor.[33]

Lorenz-type attractors illustrate the dynamic nature of data and the impossibility of knowing every potential detail. To grasp the concepts at play, an approximation is required. Edward Lorenz's simplification of the atmospheric model in 1963 using only x, y, and z was a breakthrough. Eq. (5) reduces the atmospheric change process to a differential equation:

\[
\begin{align*}
\frac{dx}{dt} &= \alpha (y - x) \\
\frac{dy}{dt} &= x(\beta - z) \\
\frac{dz}{dt} &= xy - \gamma z
\end{align*}
\]

(5)

In this case, the Prandtl number is indicated by the letter alpha, Rayleigh number by the letter beta, and geometric factor by the letter gamma.

Figure 1: Lorenz Attractor[34].

C. GIFT Block Cipher

GIFT is a lightweight encryption technique that can decrypt data in 64-bit blocks using keys of 128 or 256 bits in length. Lightweight and able to encrypt 64-bit blocks with keys of 128 or 256 bits, the GIFT block cipher algorithm was developed in 2011 by Simon and Quisqueya. Owing to its efficiency and speed, GIFT has attracted a lot of attention in recent years, making it a potentially useful tool in many fields, including the Internet of Things and mobile communications, and is built on a circular framework that utilizes add-Rotate-XOR and bit permutation operations[7].

The 64-bit block is split into four 16-bit words for the Add-Rotate-XOR operation, with each word undergoing addition, rotation, and XOR in turn. The GIFT algorithm combines several procedures to produce robust encryption in a small number of rounds.
The n-bit block (n=64,128) is separated into four bits and used as the input value for the 4-bit box in the GIFT block cipher. The boxes for the GIFT block cipher are listed in Table (1).

- The ith bit of block B in the GIFT-64/128 permutation is interchanged with the ith bit of block P64. The permutation data are presented in Table (2).

**TABLE 1. Coded Gift Box (SBOX).**

<table>
<thead>
<tr>
<th>x</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>a</th>
<th>b</th>
<th>c</th>
<th>d</th>
<th>e</th>
<th>f</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sbox(x)</td>
<td>c</td>
<td>5</td>
<td>6</td>
<td>b</td>
<td>9</td>
<td>0</td>
<td>a</td>
<td>d</td>
<td>3</td>
<td>e</td>
<td>f</td>
<td>8</td>
<td>4</td>
<td>7</td>
<td>1</td>
<td>2</td>
</tr>
</tbody>
</table>

**TABLE 2. GIF-Permutation of 64 bits.**

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

For the GIFT-64/128 algorithm, the key K (K=k7,..., k0) is used to select a combined 32-bit value (k0 and k1) for the gift. In the round key, the letters U and V are represented by the k0 and k1 keys, respectively. RK is represented as U concatenated with V (RK=UV = u15...u0v15...v0, where U=k1 and V=k0), and this is how the round key RK is written. To perform an exclusive operation with block B, the round key is first XORed with b4i+1, and then V is XORed with b4i.

\[
\begin{align*}
    b_{4i+1} &\leftarrow b_{4i+1} \oplus u_i, b_{4i} &\leftarrow b_{4i} \oplus v_i, i = 0,...,15
\end{align*}
\]

For the GIFT-128/128 algorithm, key K is used to select one of four different 64-bit values (k0, k1, k4, or k5). These values are utilized as the U and V components of the round key, where U is the result of concatenating k5 and k4 and V is the result of concatenating k1 and k0 (RK=UV = u31...u0v31...v0, where U=k5k4 and V=k1k0). When block B is XORed with a round key, U is XORed with b4i+2, and V is XORed with b4i+1.

\[
\begin{align*}
    b_{4i+2} &\leftarrow b_{4i+2} \oplus u_i, b_{4i} + 1 &\leftarrow b_{4i} + 1 \oplus v_i, i = 0,...,31
\end{align*}
\]
Constant XOR: The GIFT-64/128 and GIFT-128/128 ciphers both use the round constant $C$, which may be found in Table 3. As shown in Equation (3), block $B$ is created by combining the single-bit constants with the round constants using the XOR operation.

$$b_{n-1} \oplus b_{n-1} \oplus b_{n-2} \oplus b_{n-3}$$

$$b_{15} \oplus b_{7} \oplus b_{3} \oplus c_{1}$$

$$b_{14} \leftarrow b_{14} \oplus c_{2} \oplus b_{7} \oplus c_{1}$$

$$b_{3} \ominus c_{0} \ominus b_{2} \ominus b_{1} \ominus b_{0}$$

Equation (3)

Key $K$ ($k_{7}, \ldots, k_{0}$) is always updated in the GIFT-64/128 and GIFT-128/128 ciphers, and the round key is always generated from the original key. A right rotation operation, also known as an $i$-bit and denoted by symbol $(i)$, is part of the key schedule. The following equation is used to compute the updated key.

$$k_{j} \ll k_{i} \ll \ldots \ll k_{0} \leftarrow k_{j} \ll k_{i} \ll \ldots \ll k_{0}$$

Equation (4)

This revised explanation of the GIFT algorithm offers profound insight into its fundamental workings and mechanics, illuminating the algorithm’s singular qualities and the significant role it plays in the field of block cipher encryption.

<table>
<thead>
<tr>
<th>Rounds</th>
<th>Constants C</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 to 16</td>
<td>01 03 05 07 09 11 13 15 17 19 21 23 25 27 00</td>
</tr>
<tr>
<td>17 to 32</td>
<td>31 33 35 37 39 31 33 35 37 39 31 33 35 37 00</td>
</tr>
<tr>
<td>33 to 48</td>
<td>01 03 05 07 09 11 13 15 17 19 21 23 25 27</td>
</tr>
</tbody>
</table>

4. The Proposed System

The proposed method (CSKey) is a novel approach for generating random keys for chaotic systems and is grounded in Chaos Theory (Lozens method). A string of random numbers was generated using CSKey. By combining these random numbers with the lightweight GIFT algorithm, we were able to boost the CSKey’s speed and make a secure chaotic encryption mechanism available for use by IoT devices transmitting medical data. Figures 3 and 4 depict in greater detail how the proposed method utilized the initial values for these maps. Figure (5) below demonstrates this point.

![Integrated Chaotic-GIFT Lightweight Encryption Algorithm](image-url)

Figure 3: Integrated Chaotic-GIFT Lightweight Encryption algorithm.
5. The Metrics of Performance

Lightweight encryption techniques should be evaluated based on their performance quality. This article describes the steps used by the researchers to investigate and evaluate the GIFT algorithm with and without the proposed Chaos Secret Key. Both with and without the suggested Chaos Secret Key, these measures were done (CSKey). The proposed key will be tested in the algorithm to see how well it works compared to the standard method. When describing a wide range of internationally recognized indicators, the term "performance metrics" is commonly used to describe the indicators as a whole [36].

1) Entropy is a physical number used to quantify the degree of disorder that exists within a closed system. Uncertainty is a useful descriptor of entropy, which is why we used it here. The amount of entropy in a
system can be either greater or lower, depending on the conditions. Encryption keys, which are used for protecting data while being transferred or stored, are generated using random integers that are produced by entropy. The security value of a key is directly proportional to the quality of generated random numbers. The quality of the random key generator directly correlated to an increase in the quality of the random number generator.

2) The most popular estimation statistic for image quality is mean squared error (MSE). Because it is a comprehensive reference metric, its value should be as close to zero as is practically practicable. The same error commenced again. MSE is calculated by considering both the volatility and bias of the estimator. The variance of an estimator and the MSE are equivalent when dealing with a credible estimate. Equation shows that it uses the same measuring systems as the square root of the quantity being calculated, in this case the variance (6). MSE is the factor that leads to the development of the Root-Mean-Square Error (RMSE) or Root-Mean-Square Deviation (RMSD), which is more frequently referred to as the variance standard deviation.

\[
MSE = \frac{1}{mn} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} [f(i,j) - k(i,j)]^2
\] (6)

3) The accuracy with which a signal is represented is measured relative to the degree of distortion introduced by background noise using a statistic called the Peak Signal-to-Noise Ratio (PSNR). The difference between the two photographs was expressed as a decibel reading. The peak signal-to-noise ratio (PSNR) is typically expressed as a logarithm of the decibel scale owing to its high signal-to-noise ratio, as shown in Equation (7). This dynamic range includes not only the lowest possible quality, but also the highest possible quality in terms of the range of values that may be imagined.

\[
PSNR = 20 \cdot \log_{10} \left(\frac{MAX}{MSE}\right) - 10 \cdot \log_{10} (MSE)
\] (7)

4) An easy-to-compute metric that can be implemented across a wide range of image editing software, the Universal Quality Image Index is used to evaluate the success of an edited image.[23].

\[
Q = \frac{1}{M} \sum_{j=1}^{m} Q/j
\] (8)

5) The structural similarity index (SSIM) was determined as. This is a model that makes inferences. Here, we view visual deterioration as a modification to how we interpret an image's underlying structure. Additional fundamental perceptual truths are also supported, such as luminance and contrast masking. We refer to "structural information" as pixels that are highly dependent on one another or physically close together. Information is gleaned from the interdependencies of the image pixels that are not directly captured. It's purpose is to compare the recovered image to its source to see how close it comes.[24].

\[
SSIM(x,y) = \frac{(2\mu_x\mu_y + C_1)(2\sigma_{xy} + C_2)}{\sigma_x^2 + \mu_y^2 + C_1} \frac{(2\sigma_{xy} + C_2)}{\sigma_y^2 + \mu_x^2 + C_2}
\] (9)

6) Measuring the Spatial Correlation Coefficient (SCC): The average gain of the incoming signal correlates with the signal's angle of arrival, and thus the strength of the linear relationship between x and y can be regarded as a measure of spatial correlation.

\[
\text{Correlation} = \rho = \frac{\text{Cov}(x,y)}{\sigma_x \cdot \sigma_y}
\] (10)
7) The pace at which the total number of pixels in the cipher picture changes in response to a change in a single pixel in the plain image is known as the number of changing pixel rate (NPCR).

\[ NPCR = \frac{\sum_{i,j}D(i,j)}{W \times H} \times 100\% \]  

8) By contrasting the original and encrypted copies of an image, the Unified Average Changing Intensity (UACI) determines the extent of the difference between the two.

\[ UACI = \frac{1}{W \times H} \sum_{i,j} \left\lfloor \frac{|C1(i,j) - C2(i,j)|}{255} \right\rfloor \times 100 \] 

6. Result and Discussion

The robustness and reliability of the proposed cryptosystem were tested by a number of experiments undertaken by researchers. Tables (4) and (5) show the results of experiments and measurements designed to ensure the system's resistance to various attacks. First, offer a histogram analysis that demonstrates how the pixels in the encrypted photos are distributed consistently and how this distribution is fundamentally distinct from that of plain images. The randomness of the image and its resistance to entropy attacks can then be shown by computing its information entropy. The proposed cryptosystem reduces the correlation between adjacent pixels in the original image in a sequential fashion, as shown by the correlation coefficient. The number of pixels changing per second (NPCR) and unified average changing intensity (UACI) tests were used to analyze differential attacks. The proposed cryptosystem's private key analysis demonstrates its resistance to large-scale attacks, and it has been shown through probabilistic analysis that the same keyframe and secret keys produce vastly different encrypted keyframes from the cryptosystem. In addition, the sensitivity analysis proves beyond a reasonable doubt that recovering the original frames from a backup requires knowledge of the correct values of the secret keys. Therefore, if the secret keys are altered, there is a noticeable shift in the encrypted image. The study of the image quality further confirmed the high quality of the encrypted image. Anti-clipping analysis is used to test the robustness of a cryptosystem by simulating attacks in which data from specific blocks are removed. Finally, our cryptosystem was shown to be significantly better than the state-of-the-art in a comparison investigation.

### TABLE 4. Performance Presentation of the GIFT's Original Composition.

<table>
<thead>
<tr>
<th>Images</th>
<th>Energy-original</th>
<th>Energy encryption</th>
<th>Mean-Squared Error</th>
<th>PSNR</th>
<th>Universal Quality Image index</th>
<th>Correlation Horizontal</th>
<th>Correlation Vertical</th>
<th>Correlation Diagonal</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lena</td>
<td>7.751334</td>
<td>7.999107</td>
<td>8955.318346</td>
<td>8.609565</td>
<td>0.794425</td>
<td>0.016325</td>
<td>0.004026</td>
<td>0.005427</td>
</tr>
<tr>
<td>Baboon</td>
<td>7.69805</td>
<td>7.999219</td>
<td>8261.27478</td>
<td>8.97086</td>
<td>0.735535</td>
<td>0.018764</td>
<td>-0.000377</td>
<td>99.4481</td>
</tr>
<tr>
<td>Pepper</td>
<td>7.733452</td>
<td>7.983404</td>
<td>10059.49066</td>
<td>8.124849</td>
<td>0.605297</td>
<td>0.017228</td>
<td>0.008208</td>
<td>99.4568</td>
</tr>
<tr>
<td>Car</td>
<td>7.510458</td>
<td>7.995685</td>
<td>9106.053447</td>
<td>8.557501</td>
<td>0.747996</td>
<td>0.012635</td>
<td>0.001407</td>
<td>99.3506</td>
</tr>
<tr>
<td>Cameraman</td>
<td>7.043529</td>
<td>7.992435</td>
<td>9329.13441</td>
<td>8.439086</td>
<td>0.640315</td>
<td>0.010425</td>
<td>-0.000227</td>
<td>99.6942</td>
</tr>
<tr>
<td>Lora</td>
<td>7.183412</td>
<td>7.964609</td>
<td>12124.80885</td>
<td>7.294057</td>
<td>0.381592</td>
<td>0.023482</td>
<td>0.002406</td>
<td>99.6635</td>
</tr>
<tr>
<td>CT_image</td>
<td>6.331148</td>
<td>7.990526</td>
<td>9431.658569</td>
<td>8.335319</td>
<td>0.586687</td>
<td>0.006349</td>
<td>0.0003243</td>
<td>99.5926</td>
</tr>
<tr>
<td>Pic1</td>
<td>7.763343</td>
<td>7.998955</td>
<td>9301.81755</td>
<td>8.445125</td>
<td>0.615436</td>
<td>0.025933</td>
<td>0.013171</td>
<td>99.4174</td>
</tr>
<tr>
<td>Encode_Sele</td>
<td>6.584175</td>
<td>7.999522</td>
<td>15282.23976</td>
<td>6.283934</td>
<td>0.223356</td>
<td>0.001029</td>
<td>0.001236</td>
<td>99.6513</td>
</tr>
</tbody>
</table>

https://doi.org/10.54216/JCIM.120105

Received: December 21, 2022 Revised: February 10, 2023 Accepted: April 24, 2023
### TABLE 5. Effects of Integrated GIFT on Performance.

<table>
<thead>
<tr>
<th>Images</th>
<th>Entropy original</th>
<th>Entropy encryption</th>
<th>MeanSquared Error</th>
<th>PSNR</th>
<th>Universal Quality Image Index</th>
<th>Correlation Horizontal</th>
<th>Correlation Vertical</th>
<th>Correlation Diagonal</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lena</td>
<td>7.98076</td>
<td>7.99894</td>
<td>8949.47475</td>
<td>0.729376</td>
<td>0.202475</td>
<td>0.00085</td>
<td>99.4873</td>
<td>21.924</td>
</tr>
<tr>
<td>Baboon</td>
<td>7.69905</td>
<td>7.999157</td>
<td>8252.22654</td>
<td>0.735127</td>
<td>0.019906</td>
<td>-0.0213</td>
<td>99.2537</td>
<td>19.9766</td>
</tr>
<tr>
<td>Pepper</td>
<td>7.735852</td>
<td>7.731554</td>
<td>10169.8229</td>
<td>0.810785</td>
<td>0.065841</td>
<td>0.018334</td>
<td>99.2117</td>
<td>23.3229</td>
</tr>
<tr>
<td>Car</td>
<td>7.987247</td>
<td>7.991972</td>
<td>9174.94378</td>
<td>8.504769</td>
<td>0.718861</td>
<td>0.026684</td>
<td>99.4751</td>
<td>24.5007</td>
</tr>
<tr>
<td>Cameraman</td>
<td>7.043329</td>
<td>7.96896</td>
<td>923.33531</td>
<td>8.393362</td>
<td>0.645461</td>
<td>0.008552</td>
<td>99.6048</td>
<td>31.1613</td>
</tr>
<tr>
<td>Lora</td>
<td>7.183412</td>
<td>7.998911</td>
<td>12530.2224</td>
<td>7.260687</td>
<td>0.370736</td>
<td>0.025159</td>
<td>99.6113</td>
<td>31.0624</td>
</tr>
<tr>
<td>CT_image</td>
<td>7.337448</td>
<td>7.514283</td>
<td>9493.22376</td>
<td>8.372249</td>
<td>0.554491</td>
<td>0.017018</td>
<td>99.6231</td>
<td>31.2445</td>
</tr>
<tr>
<td>Pic1</td>
<td>7.762043</td>
<td>7.999018</td>
<td>9303.82291</td>
<td>8.414189</td>
<td>0.620233</td>
<td>0.018319</td>
<td>99.4141</td>
<td>22.1799</td>
</tr>
</tbody>
</table>

Histograms provide a visual representation of the pixel distribution in an image by plotting the number of pixels at each color intensity level. The encrypted image must have a different histogram and pixel-value distribution than the original. Figure (6) displays the unaltered, encrypted, and decrypted versions of the same photograph. Figure (7) shows the histograms of the encrypted images and keyframes for each of the three RGB components. The three encrypted images have histograms that are uniform and distinct from the keyframes.

![Figure 6: Photographic encryption tests: (a) Original Images, (b) Encrypted Images, and (c) Decrypted Images.](https://example.com/fig6.png)
Figure 7: The histogram comparison of the unencrypted and GIFT-encrypted versions of the image in its three primary colors.

Figure 8: Histogram comparison of the unencrypted source image and the GIFT-encrypted version in the primary colors.
The correlation coefficient test demonstrated the effectiveness of the proposed cryptosystem in disassociating keyframe pixels that are spatially adjacent to one another (Figure (8)). The correlation between two random variables reveals the strength and direction of their linear relationship. This enables a comparison of encrypted and unencrypted copies of the keyframe to examine the connection between adjacent pixels. Owing to the large number of possible pixel combinations in a medical keyframe, 1024 pairs of neighboring pixels were randomly chosen for correlation analysis along the x-, y-, and z-axes (Figure (9) and (10)).

Figure 9: Correlation in the three spectral components between adjacent pixels before and after encryption, in the horizontal, vertical, and diagonal planes (R, G, and B).

Figure 10: Spectral, horizontal, and vertical correlation between adjacent pixels before and after encryption (R, G, and B).
To ensure a growing fitness for real-world applications, the comparison test is a crucial demonstration of the overall efficiency of the proposed cryptosystem with respect to other state-of-the-art cryptosystems. As discussed in the preceding sections, we conducted numerous comparative experiments. Compared to other published investigations [12], [16], [19, 20], and [22-25], the results showed that our cryptosystem performed better. Here, we compare the proposed cryptosystem with state-of-the-art encryption methods and present our findings based on a wide range of experimental investigations to demonstrate its performance. Table (6) shows that when compared to other cryptosystems, the proposed system performs exactly as well (NPCR and UACI). The proposed cryptosystem can protect the privacy and security of patients while considering these benefits.

Table 6. Comparisons are based on a wide range of metrics.

<table>
<thead>
<tr>
<th>Method</th>
<th>Image size</th>
<th>NPCR analysis</th>
<th>UACI analysis</th>
<th>Sensitivity analysis</th>
</tr>
</thead>
<tbody>
<tr>
<td>[12]</td>
<td>[256,256,3]</td>
<td>99.620</td>
<td>33.450</td>
<td>Yes</td>
</tr>
<tr>
<td>[20]</td>
<td>[640,480,3]</td>
<td>99.609</td>
<td>33.465</td>
<td>Yes</td>
</tr>
<tr>
<td>[19]</td>
<td>[256,256,1]</td>
<td>99.61</td>
<td>33.50</td>
<td>Yes</td>
</tr>
<tr>
<td>[24]</td>
<td>[256,256,3]</td>
<td>99.645</td>
<td>33.467</td>
<td>Yes</td>
</tr>
<tr>
<td>[16]</td>
<td>[256,256,3]</td>
<td>99.217</td>
<td>33.405</td>
<td>Yes</td>
</tr>
<tr>
<td>[23]</td>
<td>[640,480,3]</td>
<td>99.619</td>
<td>33.477</td>
<td>Yes</td>
</tr>
<tr>
<td>[22]</td>
<td>[256,256,1]</td>
<td>99.609</td>
<td>33.463</td>
<td>Yes</td>
</tr>
<tr>
<td>[25]</td>
<td>[640,480,3]</td>
<td>99.606</td>
<td>44.486</td>
<td>Yes</td>
</tr>
<tr>
<td>Proposed</td>
<td>[256,256,3]</td>
<td>99.817</td>
<td>31.114</td>
<td>Yes</td>
</tr>
</tbody>
</table>

7. Conclusion

In conclusion, this study suggests a highly effective and trustworthy picture cryptosystem to protect the confidentiality of medical records during transmission. Sensitive patient data are protected by the proposed cryptosystem when transferred to medical facilities. The proposed system employs a dual-chaotic-map variant of the GIFT algorithm as its cryptographic foundation. This study proposes combining and sequentially applying the orbits of two 2D chaotic maps to obtain encryption keys for an improved GIFT technique. In addition, future research should investigate the feasibility of employing this image cryptosystem for purposes other than medical records. In conclusion, this study proposes a reliable image-based cryptosystem that protects sensitive medical data during transmission. In conclusion, this study presents a secure and efficient picture cryptosystem for protecting patient confidentiality during the transmission of medical records. The proposed cryptosystem has outstanding results, and it can withstand numerous attacks that attempt to determine secret keys, including differential, statistical, and exhaustive keys. Through extensive testing and security research, the proposed cryptosystem has been shown to be both faster and safer than state-of-the-art alternatives. The proposed cryptosystem protects the confidentiality of the patient records kept in the keyframes. This method not only protects patients’ confidentiality but also lessens the need for resources such as processing power, data storage, and time spent looking for information. These findings validate the superiority of our proposed cryptosystem over prior methods and demonstrate its ability to foil differential, statistical, and exhaustive attacks. Future research into access control methods and homomorphic encryption algorithms is planned to boost the efficiency of the proposed cryptosystem and pave the way for new discoveries in this area.

Funding: “This research received no external funding”

Conflicts of Interest: “The authors declare no conflict of interest.”
References


[31] M. Benssalah, Y. Rhaskali, and M. S. Azzaz, “Medical Images Encryption Based on Elliptic Curve Cryptography and Chaos Theory,” in *2018 International Conference on Smart


