An Enhanced Hybrid Chaotic Technique for Protecting Medical Images

Marwa M. Eid[*1], Shaimaa A. Hussien[2]

[1] Faculty of Artificial Intelligence, Delta University
[2] Delta Higher Institute for Engineering and Technology, Mansoura, Egypt
Emails: Marwa.3eeed@gmail.com ; Shaimaa_ateya@yahoo.com

Abstract

Medical data has attracted much interest; a quick, lossless, and secure cryptosystem is required for saving and transferring images over open networks while maintaining the image's details. This paper shows how to protect medical images with an encryption method based on hybrid chaotic maps. The proposed hybrid method is constructed to deal with problems like confusion and diffusion with a large key space. The technique uses a mix of different chaos maps for a specific set of control settings. There is a complete explanation of how encryption and decryption operations work. The security analysis results showed that the suggested cryptosystem is safe from statistical, brute force, and differential attacks. Compared to already known methods, the estimated times for encryption and decryption make it likely that the proposed scheme can be applied in real-time applications.

Keywords: Chaos Cryptography; Medical Encryption; Bogdanov map; Lorenz Map.

1. Introduction

Data security has evolved to be an essential component of the contemporary communication system because of the quick development of multimedia and network technologies [1]. Data security is necessary to maintain the data's integrity and confidentiality and to protect it from intruders and unauthorized users. There are numerous methods for concealing data, including steganography, cryptography, and watermarking [2]. Watermarking can be either visible which used for copyright protection or invisible which considered as a type of steganography which hides information inside a cover digital media. Both of steganography and cryptography are complementary, as steganography conceals the existence of the communication, whereas cryptography uses encryption to alter and obfuscate the message itself. Therefore, Steganography prevents detection of the communication's existence and cryptography stops unauthorized parties from learning the communication's content. Steganography does not change the structure of a hidden message technically, but cryptography does [3]. Cryptography is the science of encrypting and decrypting data using mathematical algorithms to make messages secret by converting understandable data into an unintelligible form (cypher message) [4]. It essentially consists of two parts: encryption and decryption. Public key cryptography and symmetric key cryptography are the two categories of cryptography algorithms [5]. These types have different issues to expatiate and different goals to be achieved. Depending on the type of application domain where data encryption is utilized, the primary objectives are identified. Being compatible with current established technologies and having the capacity to apply them in all IoT applications is the distinguishing issue with security techniques employed in cryptography. The development of a robust, secure system that achieves a balance between several needs, such as: fast processing, high accuracy, authentication, bandwidth, attacks impregnability, real time computing, efficiency, reliability, security, resistance against noise, privacy, and authorization.

Doi : https://doi.org/10.54216/JCIM.100104
Received: April 01, 2022 Accepted: July 29, 2022

Many security strategies have been created to control data security over the internet even though, to a certain extent, the internet is not safe. Although many different methods are developed and deployed to be used for data security, cryptography's main objective is to design protocols or schemes that can still carry out specific tasks in the presence of an adversary. Through using cryptography, users can communicate privately across a public network. Data encryption is a method for safeguarding artificial intelligence-based data. Since medical images are transferred over different networks, protecting them has become a crucial issue in recent years. Confidentiality, integrity, and authenticity are required for the safe transmission of medical images. Patient data may no longer be private if these images are used without permission. Additionally, if these images are susceptible to even the tiniest modification, it could lead to a misdiagnosis that threats the lives of the patients [6].

The simplest and most effective way to secure medical image security is by encryption, which transforms a plain image into an unreadable one using a secret key. No one can restore the plain image without the secret key. Image encryption has two major components: confusion and diffusion [7]. Traditional encryption algorithms are not appropriate for digital images, especially medical images, because of the significant correlation between image-pixels, large-size images, and data redundancy [8]. The reduction of correlation and redundancy was indeed the purpose of many medical image encryption techniques [9,10]. Although new methods for protecting medical images have been introduced, they could still be vulnerable to attacks. Medical images have a substantial association between adjacent pixels, so eliminating this correlation demands a permutation (scrambling) technique with a greater security level. With the rise in popularity of smart and intelligent gadgets, electronic health records, or "digital health records" as they are more commonly known, are now made, and shared online all the time to gather accurate information. Symptoms, medical history, patient-related information, and other data are typically included in electronic health records, which are kept up to date by the healthcare services concerned. Also, since COVID-19 came out, many medical images and records have been made and shared online by doctors and other healthcare workers [3, 4]. Also, in [5], the high court of Bombay denied bail to a man who had been out on interim bail for about ten months based on fake medical documents.

In [6], IBM said that the health industry had the most data breaches. Also, millions of people were affected in 2015 in different ways, which makes it hard for different research groups to figure out how their illegal exploitation is going. It is still difficult to handle the security of these documents, even if the Health Insurance Portability and Accountability Act (HIPAA) provides privacy legislation for digital health records [8]. One of the top security options for medical imaging in healthcare is encryption [9]. This technique converts the original image into cipher image format, allowing only authorized users to access its data [10]. The safety of image data is now the most important thing for communication over open networks and the internet. Image encryption protects information by changing the original image into one that is hard to understand. Image encryption has been used in many different areas, including Internet communication, telemedicine, medical science, multimedia systems, and military communication. The core principle of chaos-based encryption relies on the capacity of specific dynamic systems to generate sequences of random numbers. With these sequences, messages are encrypted. Multiple chaotic maps can improve the security of image encryption. In tackling clustering problems, the benefits include:

- Minimal complexity.
- High speed.
- Robustness.
- Higher machine utilization.
- It has improved product quality.
- It increased system reliability.
- A low number of parameters.
- Lack of local optima trapping.

In addition, the performance of meta-heuristic algorithms for finding the optimal global solution is exceptional.

Doi : https://doi.org/10.54216/JCIM.100104
Received: April 01, 2022 Accepted: July 29, 2022

2. Related Work

There has been a massive amount of work done recently in the field of data and information security. Cryptography is frequently used as the fundamental component of a security system. Authors in [11] provided a medical image encryption algorithm based on an enhanced ElGamal encryption system version. The data expansion issue is resolved, and the execution speed has increased. Also [12] presented a new medical image encryption scheme consisting of high-speed scrambling, pixel adaptive diffusion, and random data insertion. In [13] A generalised optical encryption framework based on Shearlets and double random phase encoding (DRPE) was suggested to encrypt medical images. In [14] there are a proposed encryption algorithm based on the edge maps. The algorithm relied on three major parts: bit-plane disintegration, generating a random pattern, and permutation. An encryption strategy is developed in [15] based on image segmentation and matrix multiplication. The main contribution is the throughput and processing speed. However, the algorithm's simplicity must be improved to resist intruders and attackers. The great complexity of chaotic systems allows for applying chaotic functions in many cryptosystems, which enhance the security and confidentiality of image encryption.

Novel strategies are presented in [16,17] using the modifications on Arnold's CAT Map (ACM); which is one of the popular chaotic transformations; these algorithms are introduced to overcome of the ACM periodicity. Many improvements have been applied on chaotic map such as in [18], which merge it with Josephus traversing. But processing time consumption was not taken into consideration. The algorithm presented in [19] identified that ACM was not appropriate to be utilized directly for image encryption but gives better results if it is concerned with visual cryptography (VC) scheme. Several techniques are utilized to disperse the pixels positions. Rivest Cipher 4 (RC4) was used in conjunction with the chaotic henon map to create subkeys that would encrypt each block with a different key [20]. Novel cryptography scheme provided in [21] which based on polynomial equation. However, neither the strength against attacks nor the time efficiency are examined [22]. Integrated ACM with Henon map for scattering the pixels to generate the key values consequently. Authors in [23] provided a new encryption technique, which is relied on random insertion and time delay depending on chaotic map as the key productor. Proposed enhanced chaos-based cryptographic scheme is presented in [24] based on Walsh–Hadamard transform combined with two different chaotic maps; Arnold and Tent maps. Other attempts are applied to employ multiple chaotic maps as in [25] which is combined with chaotic Discrete Fractional Random Transform (DFRNT) to improve and amplify the security level. Many different types of chaotic maps are proposed and enhanced to resolve its shortcomings such as periodicity after number of iterations and the consumed processing time. But, there are still a requirement for new construction combines more sophisticated defenses against attacks and the randomness effect. RSA is regarded as one of the most widely used encryption techniques which is discussed in [26].

RGB classic color space is almost universally used in digital image encrypting works. Unfortunately, due to the three channels' high correlation, there have been some issues with the encryption process. The output and input are frequently the same when performing an encryption operation on each individual pixel, which results in redundant cryptographic processes [27]. Thus, it is necessary to improve the temporal efficiency of RGB colour space encryption operations. There is not much research in other color spaces, authors in [27] presented a comparative study between the encryption results of RGB and non-RGB color spaces. The non-RGB color spaces: YCbCr, YIQ, HSV, and L*a*b* are almost as effective as RGB in terms of security. In contrast to RGB color space, these color spaces take less time to encrypt and decrypt data. Additionally, a comparison is done between the various 4 non-RGB color spaces to show that the YCbCr colour space encryption offers the best performance and time efficiency. A Zero Order Hold technique is developed in [28] which used as steganography tool by zooming strategy. The embedding procedure is done exclusively on rows, which results in a limitation of hidden data capacity. Some image steganography algorithms rely on compression such as JPEG steganographic techniques, [29] provides an enhancement in this area. Another algorithm is developed in [30] based on another compression scheme implementing the

Doi : https://doi.org/10.54216/JCIM.100104
Received: April 01, 2022 Accepted: July 29, 2022

absolute moment block truncation coding method. Secured sharing algorithm is introduced in [31] rely on Discrete Wavelet Transform (DWT) to encrypt shadow images. Although the pre-mentioned works and efforts have their advantages, there is still a requirement for efficient and fast strategy to achieve a satisfying and balanced results in image encryption.

3. Literature review

Maps and chaotic spatial systems are examples of functions whose outputs depend only on the value of the input. They can be used in many aspects to encrypt images. For instance, ShuTang et al. [32] took a 2D spatial map. They used critical sensitivity tests, adjacent pixel correlation analysis, key space analysis, and testing against attacks to show that the map was secure. The work of Farag Allah et al. [33], who put together a report on the effectiveness of several chaotic maps in the spatial domain, such as the Arnold cat map, Baker map, and logistic map, is also in the spatial domain. According to the report, the effectiveness of the maps in a novel encryption scheme was examined using visual, entropy, histogram, encryption quality, differential, known plain text (KPT), and chosen plain text (CPT) analysis. Temporal Chaos, the state of a secular system, can only be determined by a time index and the state of the system at the preceding index. Wang et al. [34] once used a "super-chaotic" map, which is a method of pure temporal chaos, in a proposed image encryption algorithm. This algorithm displayed strong security properties, including a large key space, high key sensitivity, and resistance to statistical analysis. Chaos-based algorithms have shown that they are good at security, complexity, performance, and speed. Chaotic maps include the following characteristics:

(1) They follow a set of mathematics or formulas that control their behavior.

(2) They are sensitive to initial conditions.

(3) They are unexpected and non-linear, which means that even a minor change can have huge effects.

(4) They seem disorganized and purely random.

(5) Typically, they result in fractal forms or patterns.

4. Materials and Methods

In this section we will present preliminaries on chaotic systems and chaos-based image encryption

A. Bogdanov map

The Bogdanov map, made by Arrowsmith et al. in 1993, is used in the suggested method to move the pixels in an image around randomly. The Bogdanov map is an area-preserving planar quadratic map. The recommended method uses the map's Symplicit shape and the fact that it can be broken up into smaller parts. The Bogdanov map is a chaotic 2D map that has to do with the Bogdanov-Takens bifurcation in the theory of dynamical systems. This two-dimensional map is conjugated with the Hénon map in its non-dissipative limit. Considering how closely it is related to the Henon area-preserving map [35]. The bifurcation of Bogdanov map is shown in figure 1.

$$\begin{aligned} \acute{u} &= u\cos\alpha - (v-u^2)\sin\alpha\,, \\ \acute{v} &= u\sin\alpha - (v-u^2)\cos\alpha\,, \end{aligned} \tag{1}$$

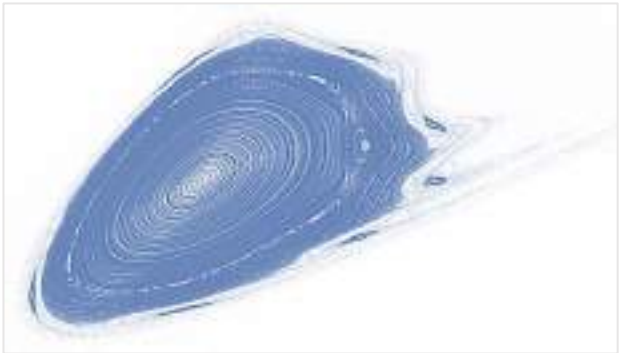

Figure 1: Bifurcation of Bogdanov map

Doi : https://doi.org/10.54216/JCIM.100104
Received: April 01, 2022 Accepted: July 29, 2022

Any second-degree area-preserving planar map, according to Henon as in Eq. (1), which may be simplified to Eq. (2) by changing the coordinates linearly, has a center (elliptic fixed point) at the origin.

The map of Bogdanov with $\varepsilon = \mu = 0$

$$\begin{aligned} \acute{x} &= x + \acute{y} \\ \acute{y} &= y + kx(x-1) \end{aligned} \tag{2}$$

When the two parts of Eq. (2) are applied to images, (x, y) stand for the coordinate positions of the pixels in the original image, while (x', y') are the resultant coordinate positions of the pixels in the altered image, and k is any positive integer ($0 < k < 4$) is such a map. The coordinate transformation between the area preserving Bogdanov map.

B. Lorenz Map

Edward Lorenz, a mathematician, and meteorologist initially explored the Lorenz system around 1960, a system of ordinary differential equations. It is noteworthy for having chaotic solutions for specific parameter values and beginning conditions. The Lorenz attractor is a collection of chaotic Lorenz system solutions. It is a dynamical system described by a nonlinear system of simple differential equations.

$$\begin{aligned} \acute{x} &= \sigma(y - x) \\ \acute{y} &= rx - y - xz \end{aligned} \tag{3}$$

The parameters are σ and r. The system enters a chaotic scope when selecting $\sigma = 10$ and $r = 28$. Because of this, given initial values for xo and yo, the system will quickly spread, and production values that are significantly different from those produced by a system are given only slightly different values for xo and yo [1]. The bifurcation of Lorenz map is shown in figure 2.

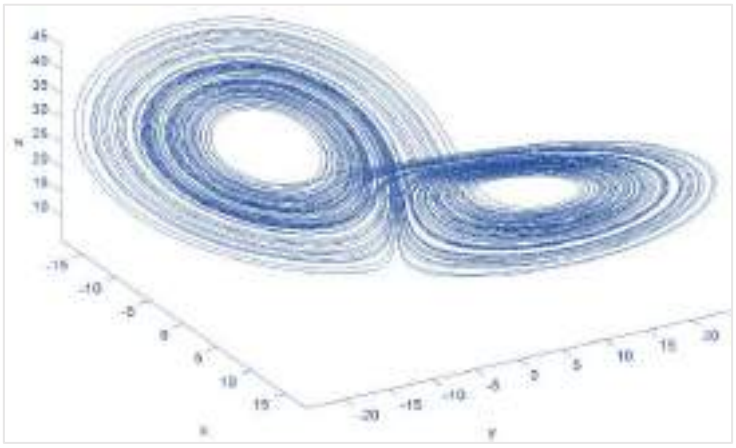

Figure 2: Bifurcation of Lorenz map

5. The Proposed System

The use of chaotic systems in multimedia encryption has recently garnered much attention. Chaos is excellent for image encryption because it has a lot of different factors that affect how it works. Because they are used as a security key during the encryption process, these parameters are critical in many ways. Minor adjustments to the system's parameter values could send it into a state of chaos. Such systems' chaotic behavior is a key building block for encryption techniques. We employ the two-dimensional Bogdanov and chaotic logistic systems in the encryption algorithm discussed in this research. The complexity of these two chaotic mapping techniques is minimal. This study proposes a system for encrypting and decrypting images that could make them more secure. To encrypt or decrypt something, you need the private medical images and set of parameters to derive the Arnold cat map. Coordinates and a Bogdanov map are used to make intimate images, which have gray pixels spread out in ways that look like pseudo-randomness. The suggested symmetric image cryptosystem is based

Doi : https://doi.org/10.54216/JCIM.100104
Received: April 01, 2022 Accepted: July 29, 2022

on chaos using the traditional confusion architecture. The permutation process changes the image pixels using the Bogdanov map. The number of iterations for the Bogdanov map depends on the total number of pixels in the plain image because the secret images have the same height and width as the plain image. Gray-level picture investigations are carried out in this paper. The architecture of the proposed system is shown in figure 3.

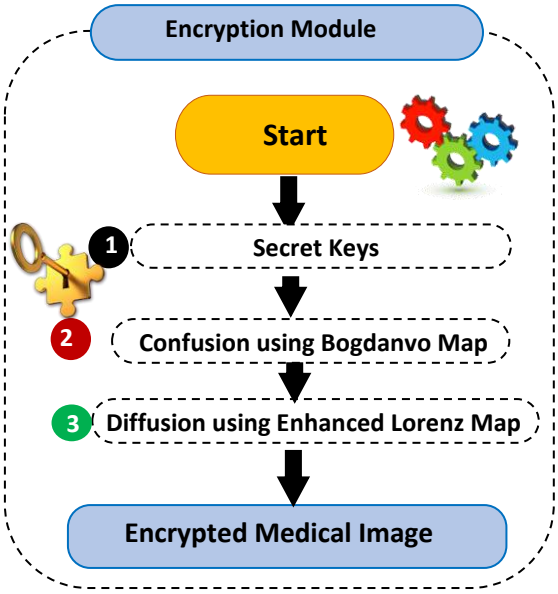

Figure 3: Main Architecture of the proposed system

The Bogdanov map (Arrowsmith et al., 1993) is used in the suggested method to move the pixels in an image randomly. The Bogdanov map is an area-preserving planar quadratic map. The recommended method uses the map's simplistic shape and the fact that it can be broken up into smaller parts. When Eqs (1) and (2) are used on images, (x, y) are the coordinate positions of the pixels in the original image, (x', y') are the coordinate positions of the pixels in the changed image, and k can be any positive integer. During the confusion stage of image encryption, the Bogdanov map is used to mix up the pixels of the image being sent in. As the positions of the pixels are changed, the relationship between the pixels in the input image gets weaker. The procedure is repeated m times to shuffle the image. Let Cs be the final image. Cs is divided into eight bit-planes, during the diffusion stage. These eight bit-planes are each individually subjected to the Bogdanov map, which is then applied n times to bit-plane Bi. The partially encrypted image Ce is then built by rearranging the scrambled bit-planes Bi. Ce is the cipher image created by running the bit-planes, which also change the value of each pixel. Ce is encrypted again with the keys made by the dyadic transform. This makes the cipher image harder to break.

Since the proposed cryptosystem is a symmetric cipher, the decryption process is the inverse of the encryption process with the same parameter vector (m, n_i , K, seed), $1 \leq i \leq 8$ and can be defined as in Eq. (4) to Eq. (9). The image decryption process is shown in Figure 2. First, the cipher image, C, is decrypted by using K and seed to get the partially deciphered image Ce. Ce is then separated into eight bit-planes, Bei, $1 \leq i \leq 8$, and the inverse Bogdanov map is applied n_i times on the bit-plane, Bei The unscrambled bit-planes of Bei are then reorganized to construct the scrambled image CS. The image CS is, however, unintelligible as the pixels are not positioned in their original position. The inverse Bogdanov map is once again applied m times on CS to unscramble the image. The resultant will be the original image, I, provided the encrypted image is not subjected to attacks on the receiving side, the secret image is generated by XORing secImgX and secImgY, which are recreated using private parameters. Inverse pixel modification is performed on the cipher image and the secret image after rounds of pixel permutations.

Doi : https://doi.org/10.54216/JCIM.100104
Received: April 01, 2022 Accepted: July 29, 2022

The result of the secret image pixel permutation in the first step is saved for subsequent steps and at each round this is inverse permuted for rounds and applied as an input to the inverse pixel modification function. The additional input is (the feedback of) the output of the inverse pixel modification function after rounds of inverse bit permutation. The decryption process is the reverse technique of the encryption process with the same parameter vector $(m, ni, K, seed)$. The inverse Bogdanov map is then applied n times to the bit-plane. The scrambled data CS is created by rearranging the unscrambled bit-planes of Bei. However, because the pixels are not in their original positions, the image CS cannot be read. To decode the image, the inverse Bogdanov map is once more applied m times on CS. If the encrypted image is not attacked, the outcome will be the original image, I.

The secret image is created on the receiving side by XORing the private parameters-recreated $secImgX$ and $secImgY$. After several iterations of pixel permutations, the cypher picture and the secret image are subjected to inverse pixel alteration. The outcome of the first step's secret picture pixel permutation is retained for later steps, and at each round, it is reverse permuted for rounds and used as an input to the function for inverting pixels. After several iterations of inverse bit permutation, the output of the inverse pixel modification function serves as the additional input (or feedback). The Bogdanov period, or the number of iterations before the image returns to its original form, is represented by the parameter p. The symmetric key is formed by the parameter vector $(m, ni, seed)$, which also regulates the confusion procedure. In the diffusion process, to avoid the negative effects of the transitional step, step one involves computing the enhanced Lorenz map and conducting c2 iterations, where c2 is constant. The steps of encryption system which shows in figure 4 is:

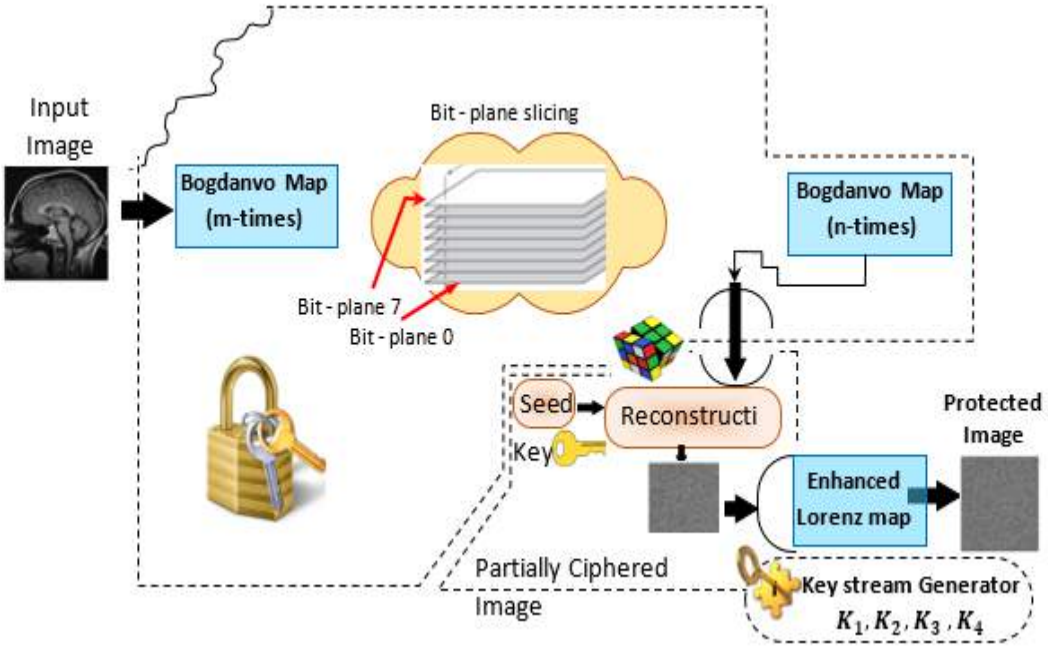

Figure 4: Steps of Encryption process

Step-1: Applying the Bogdanov map$(M,\ m)$ times on the medical image I, to create the confused image, Cs.

$$C_s = M(I, m) \quad (4)$$

Step-2: Separating the bit-planes B_i of C_s *where* Bi , $1 \leq i \leq 8$ and subjecting B_i, to the Bogdanov map n_i times, $ni \leq p$

Doi : https://doi.org/10.54216/JCIM.100104
Received: April 01, 2022 Accepted: July 29, 2022

Step-3: Establishing the partially confused image, C_e *by* employing the constructed function reorganize the permuted bit planes, B_{Si}.

$$C_e = P(M(B_{si}(Cs), n_i)) \quad (5)$$

Step-4: Computing the enhanced Lorenz map and performing c2 iterations, where c2 is constant. To get a solution of the equation, Runge-Kutta method on its fourth order is applied as [33]:

$$\begin{Bmatrix} X_{i+1} = X_i + \left(h/6\right)(K_1 + 2K_2 + 2K_3 + K_4) \\ Y_{i+1} = Y_i + \left(h/6\right)(L_1 + 2L_2 + 2L_3 + L_4) \\ Z_{i+1} = Z_i + \left(h/6\right)(M_1 + 2M_2 + 2M_3 + M_4) \end{Bmatrix} \quad (6)$$

where: h is constant step value selected to be 0.0005, the values of $Lj, kj, Mj, Nj, where\ j = 1,2,3,4,$ are computed iteratively using the following mathematical expression [33]:

$$\begin{Bmatrix} K_j = a(y_i - x_i) \\ L_j = CX_i + y_i - x_i z_i - w_{i|j=1,2,3,4} \\ M_j = X_i Y_i - \beta Z_i \\ N_j = KY_i Z_i \end{Bmatrix} \quad (7)$$

Where a, b, and c are the system parameters set in our hyperchaotic system as $(10, 8/3, 28)$ and the variable k is a control parameter determining the chaotic attractor and bifurcation set to be [0, 0.152] to produce a hyperchaotic behavior. The diffusion key is made up of the initial system variables x_i, y_i, and z_i.

Step-5: Continuously iterating Lorenz attractor where the four components of the key stream will be obtained as:

$$k_{\emptyset_n} = mod\left[round\left(\left(abs(\varphi_n)\right) - floor\left(abs(\varphi_n)\right) \times 10^{14}\right), L\right] \quad (8)$$

where: $\varphi \in \{x, y, z, w\}$ and $k_{\emptyset_n} = P\%M + 1$ is a specific shuffling to L color level and M permutation number (i.e., M=24) to the plain text pixels P .

Step-6: Performing (exclusive-OR) operation to the confused image as follows:

$$\begin{Bmatrix} C_{4\times(n-1)+1} = K_{xn} \oplus \{(p_{i4\times(n-1)+1} + K_{xn}) mod\ L\} \oplus C_{4\times(n-1),} \\ C_{4\times(n-1)+2} = K_{yn} \oplus \{(p_{i4\times(n-1)+2} + K_{yn}) mod\ L\} \oplus C_{4\times(n-1)+1,} \\ C_{4\times(n-1)+3} = K_{zn} \oplus \{(p_{i4\times(n-1)+3} + K_{zn}) mod\ L\} \oplus C_{4\times(n-1)+2,} \\ C_{4\times(n-1)+4} = K_{wn} \oplus \{(p_{i4\times(n-1)+4} + K_{wn}) mod\ L\} \oplus C_{4\times(n-1)+3,} \end{Bmatrix} \quad (9)$$

where n is the number of the system iterations and the output permutated pixels are $C_{4\times(n-1)+m}$ according to the extracted m keys (i.e., m=1,2,3,4).

Step-7: Performing step 5 till encrypting the whole data C=$\{c_1, c_2, c_3, c_{N\times N}\}$

Step-8: Rearrange the result C according to the original image data ($c_{N\times N}$) to get the completely cipher image.

Step-9: The original image can be recovered by employing the previous scenario in a reverse order.

6. Experiments and Security Analysis

A *medical database* is an integrated database that stores medical information from patients and medical facilities. Here, "medical information" refers to details like prescription drug orders for

Doi : https://doi.org/10.54216/JCIM.100104
Received: April 01, 2022 Accepted: July 29, 2022

treating patients' wounds and illnesses and the outcomes of clinical laboratory tests. We looked at the proposed method using images from the Kaggle [27]. A free database of medical shots for several medical research is Kaggle, where patients are frequently linked to a common condition (like Corona cancer), image morphology (such as an MRI or CT scan), or study area. Each image was preprocessed to 256 x 256 because they were more significant than this size. Figure 5 shows different samples of medical images from Kaggle dataset.

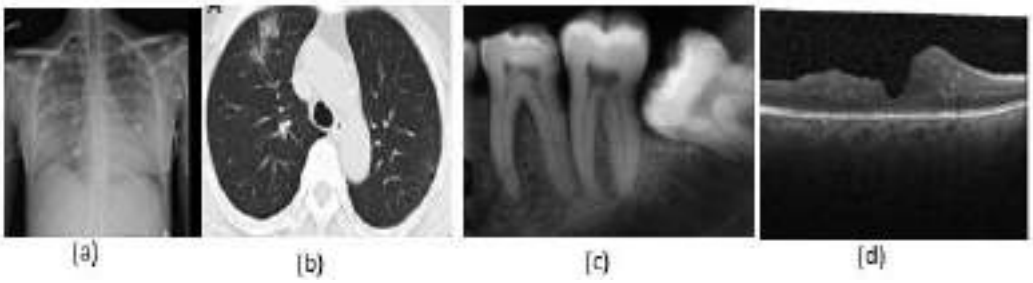

Figure 5: Samples of examined medical images from Kaggle dataset:(a) Chest X-Ray Images (Pneumonia), (b) CT COVID-19 Images, (c) Dental Images, and (d) Retinal OCT Images

The proposed system is examined through experiments to determine its security and robustness. Key space, encryption speed, and decryption speed will all play a role in deciding which cryptosystem to use. A simulation program was implemented using the **MATLAB 9.6 R2019a**: simulation environment on a PC with a 2.70 GHz Intel CoreTM i7 Duo processor, 4 GB of RAM, 360 GB of available hard disk space, and the Windows 10 operating system to show the effectiveness of the proposed approach. Finally, each simulation test has been run numerous times. The elapsed time corresponds to the mean of all trials for a certain test. A robust encryption algorithm is impervious to outsider attacks or unauthorized access. A thorough security study is necessary because of the many sorts of assaults. To investigate the effectiveness of the suggested technique, this section examines the outcomes of simulated attacks, including a statistical attack, a differential attack, a brute-force attack, and a known/chosen plaintext attack.

A. Security Analysis

Shannon defined information entropy as a mathematical theory for data communication and storage in his 1949 paper, "A Mathematical Theory of Communication" [36]. Entropy is commonly utilized to quantify disorder or unpredictability. Information entropy is used in many research areas, such as encryption and data compression. The following formula is used to define the entropy Hs of a source s:

$$H(s) = \sum_{i=1}^{2N-1} P(s_i) log_2 \frac{1}{P(S_i)} \quad (10)$$

where $P(s_i)$ stands for Si's likelihood, the source's (image's) entropy is typically lower than the ideal value for grayscale images, which is 8 [36]. Consequently, ideally, the entropy of ciphered images should be close to 8.

Table 1 contains the entropy values for the explicit and ciphered images. The ciphered image values obtained are close to the theoretical value of 8. However, if the entropy is much less than 8, the system is easy to predict, which puts its security at risk. So, there is little chance that information will get out during the encryption process, and entropy attacks cannot break the suggested digital image cryptosystem. The information entropy values found for the cipher image are very close to the ideal value. When the recommended protection method was compared to other relevant chaos-based and traditional block ciphering methods, it was found safe enough against entropy attacks.

Table 1: Samples of information entropy tests

Examined Images	Plain- image	Cipher-image

Doi : https://doi.org/10.54216/JCIM.100104
Received: April 01, 2022 Accepted: July 29, 2022

Chest X-Ray Images	7.2659	7.98835
CT COVID-19 Images	6.9427	7.98418
Dental Images	7.4462	7.99902
Retinal OCT Images	6.6960	7.98736

Fig. 6 shows the original medical and the encrypted one's histograms. The cipher image is evenly distributed and significantly different from the original template, ensuring that no significant information from the plain image escapes using the suggested technique. When comparing the protected data to the original plain image, it can be noticed that the correlation between the two is very weak, with an average correlation value of about 10-3.

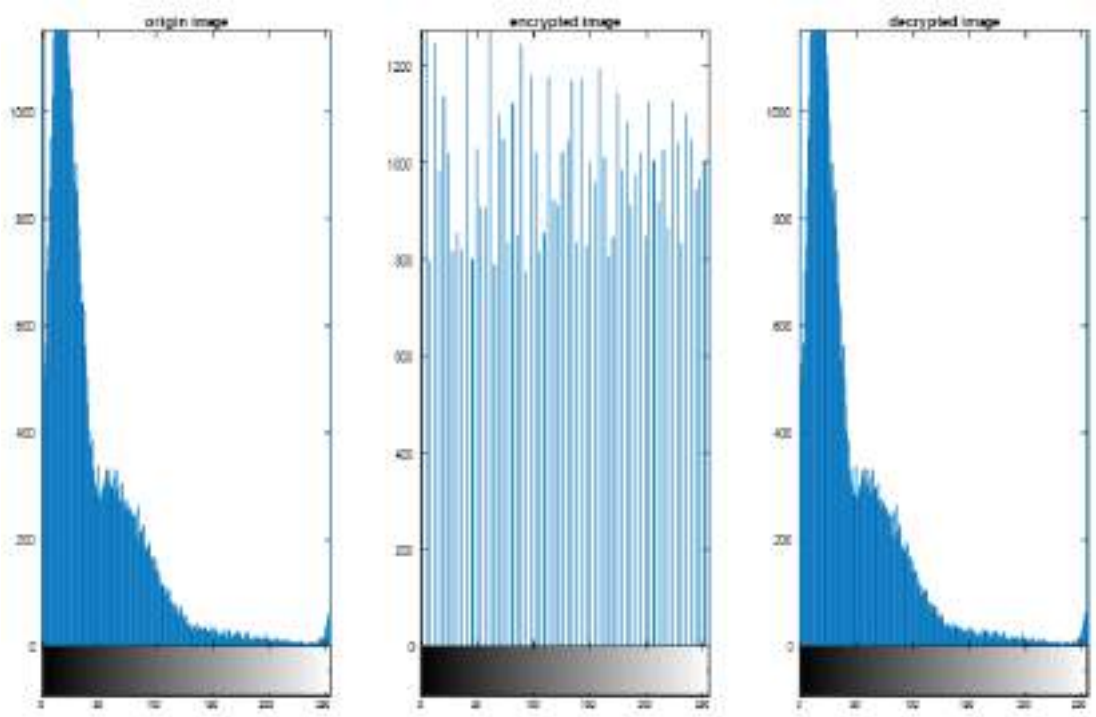

Figure 6: Histogram Analysis: (a) the histogram of the plain Chest X-Ray image, (b) the histogram of the protected image, and (c) the histogram of the decrypted image

Table 2 shows that the proposed scheme effectively eliminated the strong correlations in the three directions due to the manipulations of the proposed combination of chaotic maps. Therefore, even when dealing with extremely correlated data, such as in a medical application, it gives the cipher data resistance against statistical assault, and the estimated correlation coefficients are close to zero.

Table 2: Adjacent pixels auto-correlation analysis and comparisons

Direction	Horizontal	Vertical	Diagonal
Chest X-Ray Images	0.95693454	0.9774657	0.945142
Cipher- image from the proposed	0.000109	0.000101	0.0000091
Applying AES	0.0675	0.4621	0.1768
Applying DES	0.0073	0.0221	0.0012
Applying [x1]	0.0721	0.0512	0.0043
Applying [X2]	-0.0035	-0.0023	-0.0043

Also, the proposed method is more promising than standard ciphering methods like AES (Advanced Encryption Standard) or just using one of the chosen chaotic maps for both confusion and diffusion processes, as in [35] and [37]. Moreover, The Bogdanov period, or the number of iterations before the

Doi : https://doi.org/10.54216/JCIM.100104
Received: April 01, 2022 Accepted: July 29, 2022

image returns to its original form, is represented by the parameter p. The symmetric key is formed by the parameter vector $(m, ni, seed)$, which also regulates the confusion procedure. Thus, in the proposed system typical to IEEE floating standards, by using 10^{14} floating precision for the 7 keys thus the total key space is i.e. 10^{98} which is widely huge enough for resisting. Figure 7 shows Correlation between adjacent pixels sample of sample of protecting Chest X-Ray Images

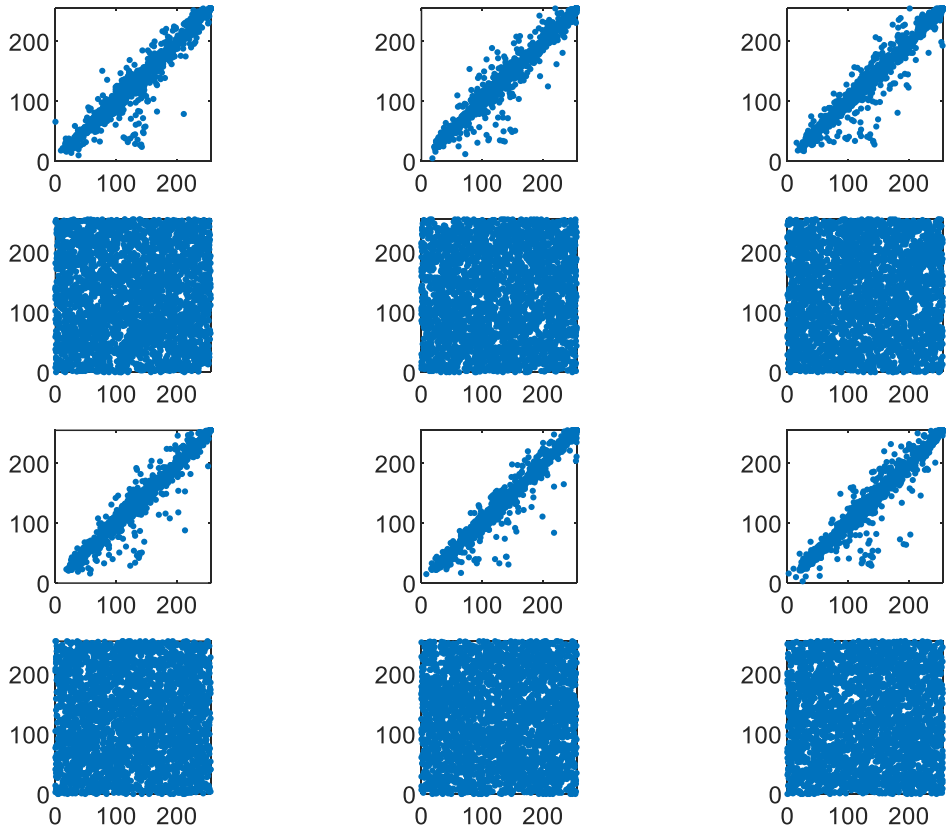

Figure 7: Correlation between adjacent pixels sample of sample of protecting Chest X-Ray Images

The proposed method to protect samples of the medical images in figure 5 are showing in figure 8 while, table 3 indicates the average protection NPCR & UACI analysis and comparison

Table 3: Average protection NPCR & UACI analysis and comparison

Applying Protection Technique for Chest X-Ray Images	NPCR	UACI
Cipher- image from the proposed	99.85972	33.5189
Applying AES	99.7617	33.4725
Applying DES	99.8504	33.3502
Applying [35]	99.8001	33.1247
Applying [37]	99.6504	33.0504

Lastly, the proposed scheme takes an average of 0.0578sec. to encrypt a medical image and 0.056sec. to decrypt it. The same dataset is employed to compare standard and related techniques. AES took 835.24 seconds to secure a single sample. Also, the proposed scheme was found to be better at keeping large amounts of data safe than similar old method.

Doi : https://doi.org/10.54216/JCIM.100104
Received: April 01, 2022 Accepted: July 29, 2022

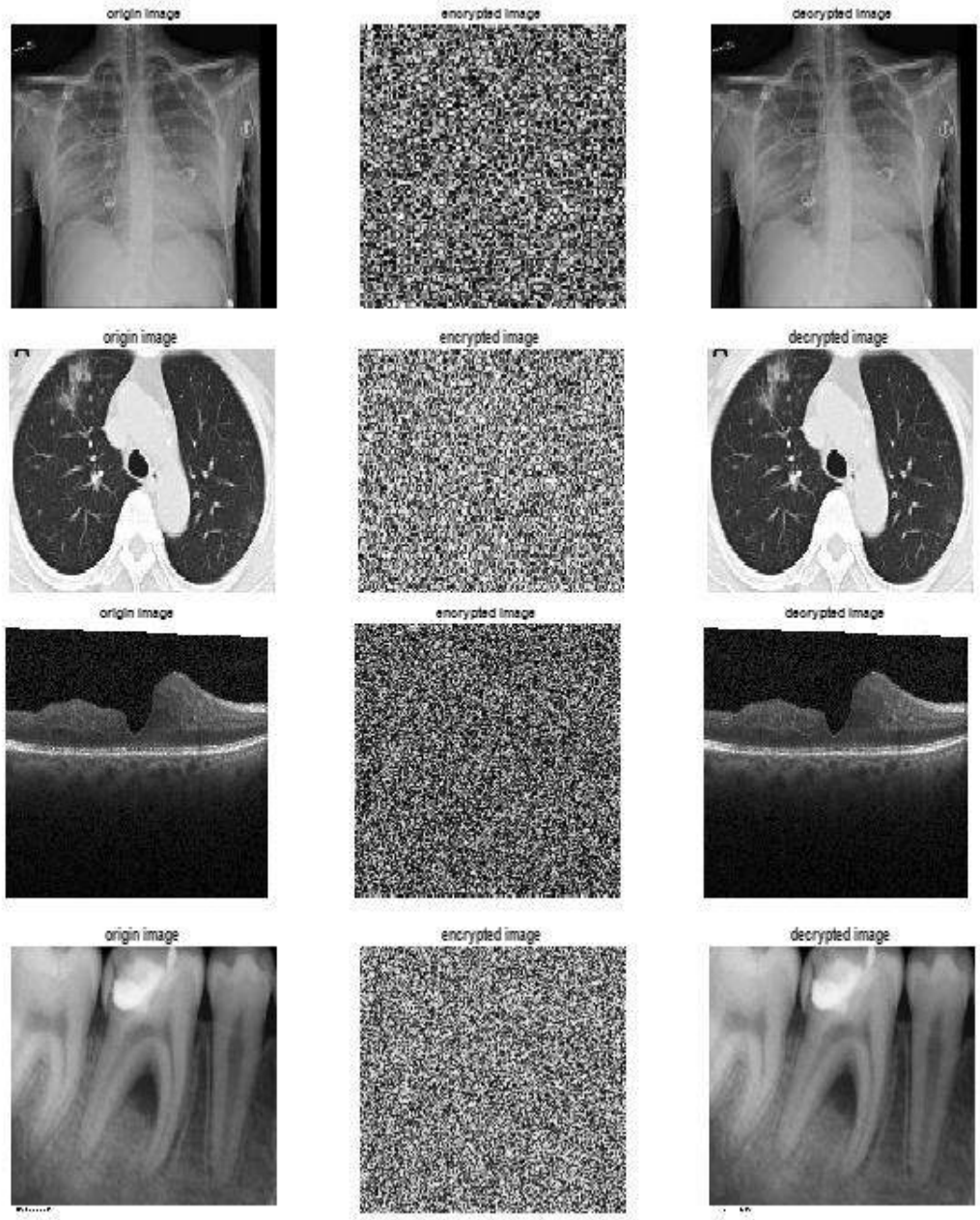

Figure 8: Applying the proposed method to protecting samples of medical images

7. Conclusion

Open networks like file shares or emails are frequently the easiest (and most effective) way to share medical images. The transmission methods of medical data put the images at risk for things like content modification, unauthorized copying, and copyright loss. This paper suggests a new way to keep medical images safe when they are sent over open communication networks. This chaotic encryption system gives more security and is easy to use. It is also strong against statistical, differential, and security analysis attacks. This technique can improve the security of encrypted data and how recognition works. The hybrid system makes use of each chaotic map's advantages. When the parameters of the 2D- Bogdanov map were changed, it produced many complicated sequences with chaotic behavior. Because it uses Lorenz mapping, a robust algorithm against known and chosen plain image attacks, the suggested method also makes it easier to meet security requirements. The improved security of the introduced scheme is confirmed through experimental testing and exams carried out with thorough analysis. Furthermore, experimental results and comparisons validated the resistance to statistical and security intrusions. As well as being able to meet online requirements, the encryption and decryption elapsed times can be further reduced by researching various chaotic maps

Doi : https://doi.org/10.54216/JCIM.100104
Received: April 01, 2022 Accepted: July 29, 2022

and using parallel computing for real-time applications. The proposed protection mechanism could be used for security-related tasks such as centrally storing medical datasets, secure Telemedicine, and healthcare applications. It can also be evaluated against various attacks and applied to different images.

Funding: "This research received no external funding"

Conflicts of Interest: "The authors declare no conflict of interest."

References

[1] Tatsuya Chuman, Warit Sirichotedumrong, and Hitoshi Kiya, Encryption-then-Compression Systems using Grayscale-based Image Encryption for JPEG Images. IEEE Transactions on Information Forensics and Security, 14 (6), 2019.

[2] Dang Ninh Tran , Hans-Jürgen Zepernick , and Thi My Chinh Chu, LSB Data Hiding in Digital Media: A Survey. EAI Endorsed Transactions on Industrial Networks and Intelligent Systems, 9, 2022.

[3] Gang Liu , Jingyuan Han , Yi Zhou , Tao Liu , and Jian Chen, QSLT: A Quantum-Based Lightweight Transmission Mechanism against Eavesdropping for IoT Networks. Wireless Communications and Mobile Computing, 2022.

[4] Chong Fu, Gao-yuan Zhang, Mai Zhu, Zhe Chen, and Wei-min Lei, A New Chaos-Based Color Image Encryption Scheme with an Efficient Substitution Key stream Generation Strategy. Hindawi Security and Communication Networks, 2018.

[5] Agus Winarno and Riri Fitri Sari, A Novel Secure End-to-End IoT Communication Scheme Using Lightweight Cryptography Based on Block Cipher. Appl. Sci. 2022.

[6] Bin Zhang, Bahbibi Rahmatullah, Shir Li Wang , Zhaoyan Liu, " A plain-image correlative semi-selective medical image encryption algorithm using enhanced 2D-logistic map", Multimedia Tools and Applications, 2022.

[7] J. Chen, L. Chen, L. Yu, and Z. Zhu, "Medical image cipher using hierarchical diffusion and non-sequential encryption," Nonlinear Dyn., 96 (1), 301–322, 2019.

[8] G. Ke, H. Wang, S. Zhou, and H. Zhang, Encryption of medical image with most significant bit and high capacity in piecewise linear chaos graphics. Measurement, 135, 385–391, 2019.

[9] A. Belazi, M. Talha, S. Kharbech, W. E. Xiang, and S. Member, Novel Medical Image Encryption Scheme Based on Chaos and DNA Encoding. IEEE Access, 7, 36667–36681, 2019.

[10] Z. Mishra and B. Acharya, High throughput and low area architectures of secure IoT algorithm for medical image encryption. J. Inf. Secure. Appl., 53, 102533, 2020.

[11] P. Suhasini and S. Kanchana, Enhanced Fractional Order Lorenz System for Medical Image Encryption in Cloud-Based Healthcare Administration. International Journal of Computer Networks and Applications (IJCNA) , 9, 2022.

[12] Z. Hua, S. Yi, and Y. Zhou, Medical image encryption using high-speed scrambling and pixel adaptive diffusion. Signal Processing, 144, 134–144, 2018.

[13] M. Chen, G. Ma, C. Tang, and Z. Lei, Generalized optical encryption framework based on Shearlets for medical image. Opt. Lasers Eng., 128, 2020.

[14] Jaishree Jain and Arpit Jain, Securing E-Healthcare Images Using an Efficient Image Encryption Model. Scientific Programming, Volume 2022.

[15] Musbah A, Ziad A, and Ammar A, RGB color image encryption decryption using image segmentation and matrix multiplication. Int J Eng Technol, 7, 104–107, 2018.

[16] Deniz E and Nursin C, An efficient image encryption algorithm for the period of Arnold's CAT map. Int J Intell Syst Appl Eng., 6, 80–84, 2018.

[17] S. H. Murad, A. M. Gody, and T. M. Barakat, "Enhanced Security of Symmetric Encryption Using Combination of Steganography with Visual Cryptography," arXiv preprint arXiv:1902.11167, 2019.

[18] Xingyuan W, Xiaoqiang Z and Yingqian Z, An image encryption algorithm based on josephus traversing and mixed chaotic map. IEEE Access, 6, 23733–23746, 2018.

[19] Reem H and Huda A, Cipher secret image using hybrid visual cryptography. ARPN J Eng. Appl Sci., 13, 1015–1021, 2018.

Doi : https://doi.org/10.54216/JCIM.100104

Received: April 01, 2022 Accepted: July 29, 2022

[20] Dena A and Salah A, Image encryption algorithm based on Rc4 and henon map. J Theor Appl Inf. Technology, 96, 7065–7076, 2018.
[21] Kavitha K and Vidhya P, Color image encryption: a new public key cryptosystem based on polynomial equation. Springer Nat Switz Proc Int Conf Ismac Comput Vis Bio-Eng 30, 69–78, 2019.
[22] Pranjali S, Shruti P, Surabhi S and Anita L, An image cryptography using henon map and arnold cat map", Int Res J Eng Technology, 5, 1900–1904, 2018.
[23] Xiaoling H and Guodong Y, An image encryption algorithm based on time-delay and random insertion. Entropy, 20(974), 2018.
[24] Sneha S, Syam S and Ashok K, A chaotic colour image encryption scheme combining Walsh-Hadamard transform and Arnold-Tent maps. J Ambient Intell Human Comput., 2019.
[25] Ankita B, Mohit D, Dua Shelza (2018), A novel approach to encrypt multiple images using multiple chaotic maps and chaotic discrete fractional random transform. J Ambient Intell Human Comput. 10, 3519–3531,2018.
[26] Yonglin Xu, Shaofei Wu, Mingqing W, and Yuntao Z , Design and implementation of distributed RSA algorithm based on Hadoop. J Ambient Intell Human Comput., 2018.
[27] https://www.kaggle.com/datasets, last access on Jan.,2023.
[28] Shashidhara N and Usha, A Video steganography using zero order hold method for secured data transmission. Int J Comput Appl., 176, 44–48, 2017.
[29] Bao Z, Guo Y, Li X et al., A robust image steganography based on the concatenated error correction encoder and discrete cosine transform coefficients. J Ambient Intell Human Comput., 2020.
[30] Yung Y, Chih H, Sin Y, and Hsin L, Data hiding method for AMBTC compressed images. J Ambient Intell Human Comput, 2018.
[31] Nadeem Ahmed , Zhongliang Deng, Imran Memon , Fayaz Hassan , Khalid H. Mohammadani , and Rizwan Iqbal, A Survey on Location Privacy Attacks and Prevention Deployed with IoT in Vehicular Networks. Wireless Communications and Mobile Computing Volume 2022.
[32] Fuyan Sun, Shutang Liu, Zhongqin Li, Zongwang Lu, A novel image encryption scheme based on spatial chaos map, Chaos, Solitobs & Fractals, 38(3), 631-640, 2008.

[33] O. S. Faragallah et al., Investigation of Chaotic Image Encryption in Spatial and FrFT Domains for Cybersecurity Applications. IEEE Acess, 42491- 42503, 2020.
[34] Wang et al., A novel Encryption Algorithm Based on DWT and Multichaos Maping.Embedded Systems for Mobile Sensors, Volume 2016.

[35] Subashini, V. J., and S. Poornachandra, Chaos based image encryption using Bogdanov map. Journal of Computational and Theoretical Nanoscience, 14 (9),4508-4514, 2017.
[36] Shannon, Claude Elwood., A mathematical theory of communication. The Bell system technical journal 27(3), 379-423, 1948.
[37] Zhang, Jian., An image encryption scheme based on cat map and hyperchaotic lorenz system. 2015 IEEE International Conference on Computational Intelligence & Communication Technology. IEEE, 2015.

Doi : https://doi.org/10.54216/JCIM.100104
Received: April 01, 2022 Accepted: July 29, 2022