



# IEFHAC: Image encryption framework based on hessenberg transform and chaotic theory for smart health

Aiman Jan<sup>1</sup> · Shabir A. Parah<sup>1</sup>  · Bilal A. Malik<sup>2</sup>

Received: 17 January 2021 / Revised: 21 March 2021 / Accepted: 9 February 2022 /  
Published online: 9 March 2022

© The Author(s), under exclusive licence to Springer Science+Business Media, LLC, part of Springer Nature 2022

## Abstract

Smart cities aim to improve the quality of life by utilizing technological advancements. One of the main areas of innovation includes the design, implementation, and management of data-intensive medical systems also known as big-data Smart Healthcare systems. Smart health systems need to be supported by highly efficient and resilient security frameworks. One of the important aspects that smart health systems need to provide, is timely access to high-resolution medical images, that form about 80% of the medical data. These images contain sensitive information about the patient and as such need to be secured completely. To prevent unauthorized access to medical images, the process of image encryption has become an imperative task for researchers all over the world. Chaos-based encryption has paved the way for the protection of sensitive data from being altered, modified, or hacked. In this paper, we present an Image Encryption Framework based on Hessenberg transform and Chaotic encryption (IEFHAC), for improving security and reducing computational time while encrypting patient data. IEFHAC uses two 1D-chaotic maps: Logistic map and Sine map for the confusion of data, while diffusion has been achieved by applying the Hessenberg household transform. The Sin and Logistic maps are used to regeneratively affect each other's output, as such dynamically changing the key parameters. The experimental analysis demonstrates that IEFHAC shows better results like NPCR ranging from 99.66 to 100%, UACI of 37.39%, lesser computational time of 0.36 s, and is more robust to statistical attacks.

**Keywords** Smart cities · Medical diagnosis · Security · Computational complexity · Image encryption

---

✉ Shabir A. Parah  
shabireltr@gmail.com

<sup>1</sup> Department of Electronics and Instrumentation Technology, University of Kashmir, Srinagar, India

<sup>2</sup> Department of Electronics and Communication Engineering, Institute of Technology, University of Kashmir Zakoora, Srinagar, India

## 1 Introduction

Smart cities are equipped with smart service delivery systems to make life more comfortable. One of the important characteristics of smart cities is the e-Health ecosystem which can be defined as a collaboration of organizations, governments, individuals, and the use of digital innovation to bring about revolutionary changes in the way healthcare services are delivered [4]. In smart cities, networked technology-based methods can be implemented to prevent and control crises like the Covid-19 pandemic [44]. One of the major areas of innovation includes improvement in the service delivery of smart healthcare systems [20]. Artificial Intelligence (AI) and IoT-based solutions along with proper security frameworks can ensure the efficient implementation of smart health infrastructures [26]. However, together with numerous benefits, the system must assure security, privacy, and confidentiality of medical records [15]. A significant portion of patient data is in the form of images, like, X-ray images, MRI images, etc. Such records have to be transmitted in a confidential and secure environment [23].

Transferring medical images via an insecure network may result in image alteration and can lead to the wrong diagnosis of a patient which could result in a lethal health problem. Despite a tremendous emphasis on developing security solutions for secure information exchange, there had been certain instances where confidential medical records were hacked and modified. For example, on April 17, 2020, Oakland country suffered a leak of a non-public map that includes information about positive Coronavirus cases [10]. Another, data breach has been recorded on April 18, 2020, in which a 16-year old hacker hacks the medical data of Mandrid health service and releases the health information about a politician (who was Coronavirus positive), on his Twitter and Instagram account [11]. As per the widely recognized Protenus breach barometer, more than 41 Million electronic patient record breaches were reported in the first eleven months of the year 2020 alone [1]. The Internet of Things (IoT), which is a new way of controlling the environment [5], is too, not free from security breaches [55]. As IoT provides a common platform for interacting images, video, web browsing, financial transactions, health information, etc. [48], the data collected and managed through IoT is stored in the cloud and each interactive action is completely dependent on the internet as such vulnerable to security threats.

Therefore, the development of a highly secure data transmission mechanism is the need of the hour. Various technologies used to achieve this objective include cryptography and steganography [52, 54]. Cryptography encrypts the data and presents it in an inconceivable manner [29]. Encryption of sensitive information can be done using standard methods, like, Data Encryption Standard (DES), Advanced Encryption Standard (AES), and Rivest Shamir Adleman algorithm (RSA) [31]. These techniques use the secret key or public key to encrypt the data or information. DES and AES have the symmetric key while RSA uses the asymmetric key for the encryption and decryption process [37]. Using standard encryption methods, we have a limitation of the key lengths with a bulk of digital data and thus are more prone to attacks. So, the standard methods are less reliable and insecure methods for encryption purposes. Encryption technique based on chaos theory overcomes the limitation of standard techniques and results in providing good security to the data being transmitted through an insecure network [38]. Chaotic encryption techniques use the initial keys for data encryption. Keys used for encryption are very sensitive to initial conditions, that is, a minute or a bit change in keys results in altogether different values [27].

One of the important parameters of a cryptographic scheme is computational complexity. The computational complexity attains more importance while communicating critical

information like patient data etc. Several encryption methods based on chaos theory have been proposed [17, 25, 30] to improve the security of the data. The authors in [30] use the information embedding approach to secure the hidden information, though this approach along with chaotic theory provides good robustness to various attacks, however, the computational complexity of the scheme is high. The authors of [25] review various encryption algorithms and conclude that for real-time applications low computationally complex algorithms are needed. In [17] a Two-dimensional Logistic-Sine-coupling map has been reported. The authors demonstrate that the scheme has better ergodicity and better security. Although the reported techniques provide better security than the standard encryption techniques in terms of security but take more time for algorithm execution. Therefore, there is a need for the development of secure and reliable chaos based algorithms that have less time complexity.

In this paper, we present the IEFHAC method which is a secure and computationally efficient image encryption scheme based on Hessenberg transformation and Chaotic theory. The scheme uses chaotic maps for confusion and Hessenberg transform for diffusion. IEFHAC has 99.66% - 100% NPCR value, 37.39% UACI value, and 0.36 s computational time value. Therefore, the method is highly robust to statistical attacks.

The main contributions of the proposed work are:

- i. A secure image framework for image encryption IEFHAC has been proposed.
- ii. The presented framework is highly secure with 99.66 to 100% NPCR value and 37.39% UACI value and can resist statistical attacks.
- iii. The presented algorithm is computationally efficient with an encryption and decryption time of 0.34 and 0.02 s respectively.

The rest of the paper is organized as follows. Section 2 presents a detailed literature review. Section 3 highlights the need for a data security frame. Section 4 and section 5 introduce the preliminaries of chaotic maps and Hessenberg transformation respectively. A detailed description of the proposed technique is provided in Section 6. Section 7 presents the simulation results and at last, the paper ends with concluding comments in Section 8.

## 2 Related work

Image encryption based on DES, AES, RSA uses the image as a binary data stream that can result in image specification loss [31]. Chaos-based methods use the structure of the algorithm and the performance of chaos theory. Many such approaches could be seen in [30, 40, 51]. In different ways, various chaos-based encryption techniques have been proposed [12, 21, 22, 42]. There are several algorithms where either one or more maps have been used to encrypt the data like in [7], where a chaos-based encryption scheme has been presented. The method has been tested on both standard as well as medical images but has poor security. QR code-based image encryption technique is proposed in [19] where only the grayscale images have been used for the test purpose. A pixel permutation and chaotic map based image encryption technique has been presented in [2]. The scheme has not been evaluated for unified average change intensity (UACI), a well-known objective quality indicator. Pseudo-random number sequence (PRNS), Arnold permutation, and AES technique-based encryption methods have been implemented in [3]. The technique has been divided into two stages where bit-level permutation and block diffusion have been implemented to encrypt the image. The scheme can

be further improved to show good security values with less time complexity. A chaotic map based image encryption technique could be seen in [39], in which Piece-Wise Linear Chaotic Map (PWLCM) has been used to permute and diffuse the pixels remaining after blocking the image into  $2 \times 2$  size. The scheme has been tested only on grayscale images and has not been able to provide good security results with less time complexity.

Logistic map based chaotic encryption and embedding technique have been proposed in [36] where the basic logistic map is modified to increase the range of the control parameter. Although the algorithmic structure comes up with a good solution but lacks enhancing the security as evident from evaluated parameters. A multiphase image encryption scheme based on chaos theory is presented in [13]. The technique has been divided into two phases: the shuffling phase and the masking phase. The scheme uses a piecewise linear chaotic map and linear approximation technique in the masking phase. The structure of the algorithm offers good encryption techniques, but the method can be further improved to enhance the security results with less computational complexity. A 3D chaos theory-based image encryption technique has been put forth in [53]. In this, a 3D cat map and pixel frequency have been applied to the image for encryption in a secure way. This technique however has tremendous scope for improvement to achieve better security. Another, 4-D chaotic circuit based image encryption design has been presented [46] to provide security to the transmitting image. The technique has developed a simple algorithm to produce a secure framework, but, can be improved further to increase security values. One more, image encryption based data hiding method has been introduced [28] in which data hiding is done by using comprehensive sensing and discrete fourier transform. In order to encrypt the data Arnold transform has been used to scramble the bits. The proposed algorithm is able to secure data. But, the scheme has used the frequency domain method, thus, has made the algorithm complex.

All the above-mentioned algorithms use only one chaotic map that results in poor security of the secret information being transferred to the receiver. To improve the security of data many encryption techniques utilizing two maps could be seen in the literature. In [14], a privacy-preserving cryptosystem using two chaotic maps has been presented to provide security to the Internet of things (IoT) E-healthcare system. Zaslusky and logistic chaotic maps have been used for encrypting data. However, this method is computationally complex. A similar approach using two chaotic maps could be seen in [18]. Njitacke et al. [34], have presented an image encryption method to protect biomedical images from thefts. The framework has controlled coexisting attractors with two chaotic pair attractors and one periodic pair for improving coupling strength. Though, the technique has improved security to the biomedical images. However, can be improved to get better NPCR value. Another chaotic map based image encryption scheme has been given in [47] to provide security to medical images during transmission. The scheme has used a 2-D trigonometric map using Logistic, Sine, and Cosine maps. Although, the method has been able to enhance security than the standard encryption methods. But, can be enhanced further to upgrade security values. A new chaos theory-based data encryption and embedding technique [24] has come up with a new way of presenting the maps to encrypt the data. In this, the logistic map and tent map have been combined in an alternative manner. The technique gives a glimpse of using different maps in an effective way to encrypt data. The method has been shown to pass various randomness tests.

A thorough survey of literature led us to conclude that using two maps is a good approach to improve security because it reorders data more randomly and cracking of two maps with more than two initial control parameters or initial conditions is difficult. A critical analysis of state-of-the-art techniques [2, 3, 13, 14, 18, 28, 34, 36, 39, 46, 47, 53], reveals that there is a

need of developing a more secure solution that is computationally efficient and which applies to both grey as well as color images. Towards this end, we provide an efficient solution, IEFHAC which is an image encryption framework based on Hessenberg transform and Chaotic theory. We show that the proposed scheme is more secure than state-of-the-art schemes and is computationally efficient.

### 3 Need for a security framework for healthcare data

The Covid-19 pandemic has put the world in difficult times. As of 16th January 2021, COVID-19 confirmed deaths 2,03,21,06 deaths worldwide [50]. A proper diagnosis while keeping a physical distance is the need of the hour. In such a scenario the use of smart healthcare is assisting the radiologists and other front-line workers to help prevent possible breakdown of healthcare facilities. This mechanism uses the internet as a medium for interaction and transmission of significant patient data. Medical imagery like Computed Tomography (CT) scans and X-ray imagery are of significant use for diagnosing COVID-19 patients. Such image data is frequently exchanged through the internet on a smart health platform. However, sharing critical personal patient information is quite risky as healthcare data breaches are exponentially increasing throughout the world. Thus, there is a need of securing this patient information (Medical imagery) to ensure secure and attack-free communication of critical data. Towards this end, we have developed an efficient image encryption solution IEFHAC for encrypting the medical imagery and hence allowing secure transfer of data which could be quite useful under testing times of Covid-19.

### 4 Cryptographic encryption based on chaotic maps

Encrypted data using chaotic maps appear to be raw, noise, or distortion and its behavior is unpredictable. Related behavior of cryptography and chaos theory has made its place for secure data transmission via an insecure network. Standard encryption techniques and chaotic encryption techniques show almost similar behavior like its sensitivity to initial conditions, random behavior, and wobbly phases but the only difference is the encryption transformation definition in phase space [35]. Cryptography is defined on a finite set of integers, while as, the chaotic system is defined on a set of real numbers. The general model for encryption is confusion and diffusion [43] shown in Fig. 1.

Confusion permutes the pixels of an image with chaotic maps whereas diffusion substitutes pixel values of an image with suitable values.

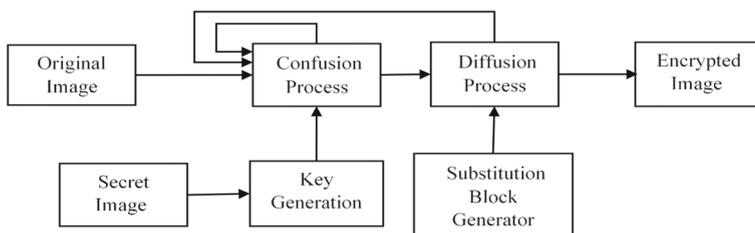


Fig. 1 General Model for Image Encryption [43]

#### 4.1 Encryption based on logistic map

The Logistic map is the simplest and the easiest encryption technique [25, 27, 33, 41]. It is a function of a nonlinear system generated by iterating the equation shown in Eq. 1 up to  $(x-1)$ . The map shows the chaotic behavior in the range of  $x_0 \in [0,1]$  for an initial condition  $[x_0]$  and control parameter  $r \in [0,1]$ .

$$x_{n+1} = r * x * (1 - x_n) \quad (1)$$

#### 4.2 Encryption based on sine map

A Sine map is another chaotic encryption map [35]. The iteration from  $[0, x-1]$  generates the random values based on Eq. 2. In this map, the control parameter  $\mu$  can be any real positive number and initial condition  $x_0 \in [0,1]$ .

$$x_{n+1} = \mu * \sin(\pi * x_n) \quad (2)$$

#### 4.3 Bifurcation diagram

Bifurcation shows the behavioral change of the system as the change of the parameter. The bifurcation plot draws phase lines for various parameter values. It is a sudden change in the qualitative global features of a system as the parameter changes. A small change in a system parameter leads to a large and quantitative change in the systems' behavior. Bifurcation in a dynamical system is a sudden quantitative change as a parameter is varied continuously. Here, quantitative is not the location of a fixed point but the change in the number of fixed points or stability that is a sudden qualitative change in the overall global behavior of the system. The bifurcation plot for the Logistic map and Sine map is shown in Figs. 2 and 3. Bifurcation of the Logistic map shows that the system behaves randomly in the range of  $[3.57, 4]$ . While the Sine map's bifurcation diagram shows random behavior from less than 0.5.

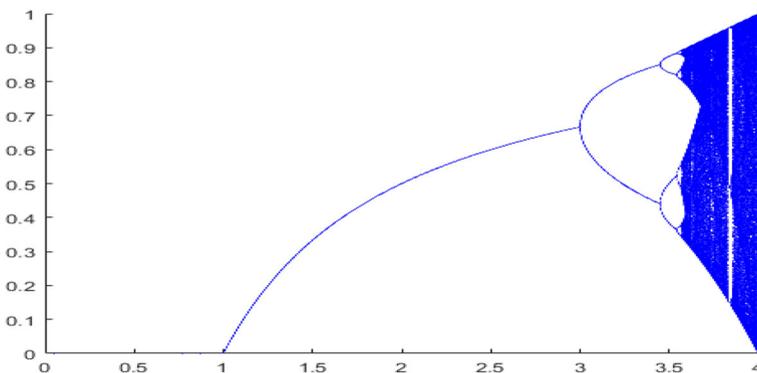


Fig. 2 Bifurcation Plot of the Logistic Map

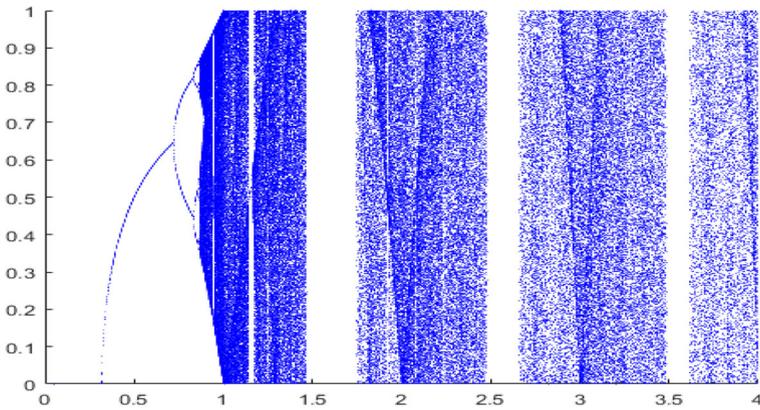


Fig. 3 Bifurcation Plot of the Sine Map

### 4.4 Lyapunov exponent

Quality of chaos is described by the sensitive dependence on the initial conditions. A small change in the initial condition leads us to different dynamic values. Chaotic exponent divergence is shown by the Lyapunov exponent. A Lyapunov exponent is a number that tells us how sensitive a system is and estimates the behavior of the chaotic system. So, it gives us more information about whether the system has a butterfly effect or not. The Lyapunov exponent for both the Logistic map and Sine map is shown in Figs. 4 and 5. The diagram indicates that the maps are good for the encryption purpose of transmitted data via an insecure network after processing.

## 5 Hessenberg transformation using household matrix

The concept of Hessenberg was given by Karl Hessenberg and the method was entitled to his name. Hessenberg Transformation (HT) is a change in a square matrix from one form to another form with different values [6, 45, 49]. The resultant matrix could be either a square matrix

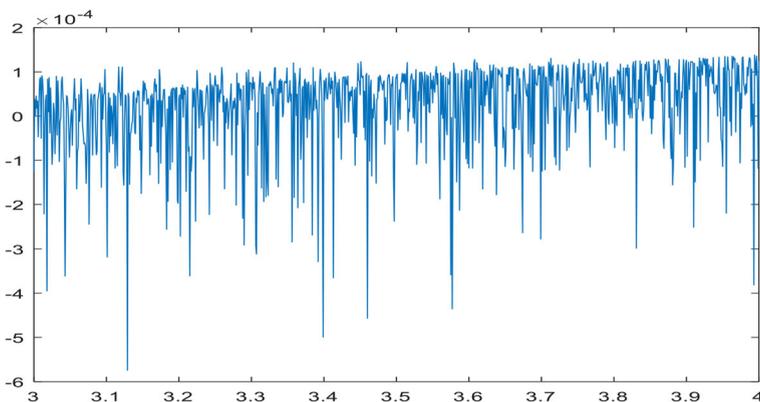


Fig. 4 Lyapunov Exponent of the Logistic Map

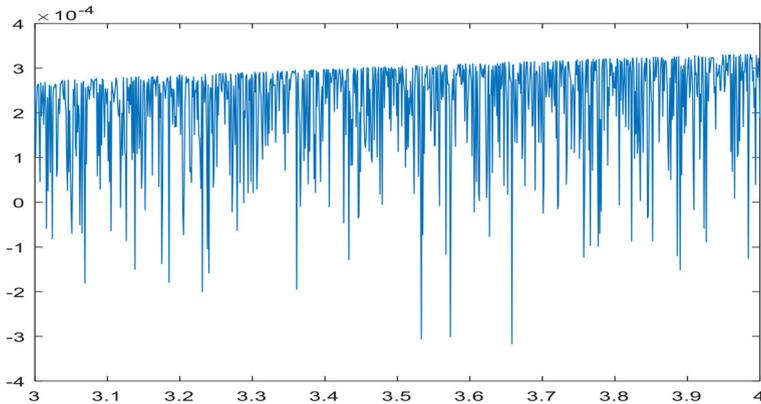


Fig. 5 Lyapunov Exponent of the Sine Map

having elements equal to zero below the first sub-diagonal, called the upper Hessenberg matrix, or the square matrix having elements equal to zero above the first super-diagonal, called lower Hessenberg matrix. Any square matrix ‘A’, can be converted to a Hessenberg matrix ‘H’ by multiplying household matrix ‘U’ and its transpose, in the manner displayed in Eq. 3.

$$H = U^T A U \tag{3}$$

Where,  $U^T U = I$  (4)

The household matrix is an orthogonal matrix [32, 33] that satisfies the condition shown in Eq. 4. The household matrix can be calculated by the approach shown in Eq. 5.

$$U = I - 2W W^T \tag{5}$$

Where ‘I’ is an identity matrix,  $W = \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ \vdots \\ x_n \end{bmatrix}$  and  $W^T = [x_1 \ x_2 \ x_3 \ \dots \ x_n]$  (6)

To form vector ‘W’, there is a need for determining  $x_0$  that can be calculated by the method shown in Eq. 7,  $a_{ji}$  are the elements of a symmetric matrix. The computation of H is described in Example 1.

$$x_1 = 0, x_2 = \frac{a_{21} - \alpha}{2r}, \text{ and } x_n = \frac{a_{n1}}{2r} \text{ for each } n = 3, 4, \dots, n \tag{7}$$

$$\text{Where, } \alpha = -\text{sign}(a_{21}) \sqrt{\sum_{j=2}^n a_{j1}^2} \tag{8}$$

$$\text{and, } r = \sqrt{\frac{1}{2}(\alpha^2 - a_{21}\alpha)} \tag{9}$$

**Example 1** Consider a matrix,  $A = \begin{bmatrix} 1 & 5 & 7 \\ 4 & 0 & 6 \\ 3 & 3 & 1 \end{bmatrix}$  and symmetric matrix,  $S = \begin{bmatrix} 1 & 4 & 3 \\ 4 & 1 & 2 \\ 3 & 2 & 1 \end{bmatrix}$  to find the Hessenberg matrix by using household transformation.

To find the household matrix (orthogonal matrix), we have to find out the values of  $x_1, x_2,$  and  $x_3$ .

Here,  $x_1 = 0, x_2 = -\frac{1}{\sqrt{10}},$  and  $x_3 = \frac{3}{\sqrt{10}}.$  Thus,  $W = \begin{bmatrix} 0 \\ -\frac{1}{\sqrt{10}} \\ \frac{3}{\sqrt{10}} \end{bmatrix}$  and

$$W^T = \begin{bmatrix} 0 & -\frac{1}{\sqrt{10}} & \frac{3}{\sqrt{10}} \end{bmatrix}.$$

There, the household matrix can be calculated using Eq. 5 i.e.,

$$U = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} - 2 \begin{bmatrix} 0 \\ -\frac{1}{\sqrt{10}} \\ \frac{3}{\sqrt{10}} \end{bmatrix} \begin{bmatrix} 0 & -\frac{1}{\sqrt{10}} & \frac{3}{\sqrt{10}} \end{bmatrix}$$

$$U = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0.8 & 0.6 \\ 0 & 0.6 & -0.8 \end{bmatrix} \text{ and } U^T = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0.8 & 0.6 \\ 0 & 0.6 & -0.8 \end{bmatrix}$$

Hence, the upper Hessenberg matrix using household can be calculated by Eq. 3 i.e.,

$$H = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0.8 & 0.6 \\ 0 & 0.6 & -0.8 \end{bmatrix} \begin{bmatrix} 1 & 5 & 7 \\ 4 & 0 & 6 \\ 3 & 3 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0.8 & 0.6 \\ 0 & 0.6 & -0.8 \end{bmatrix}$$

$$H = \begin{bmatrix} 1 & 5 & 7 \\ 5 & 1.8 & 5.4 \\ 0 & -2.4 & 2.8 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0.8 & 0.6 \\ 0 & 0.6 & -0.8 \end{bmatrix}$$

$$H = \begin{bmatrix} 1 & 8.2 & -2.6 \\ 5 & 4.68 & -3.24 \\ 0 & -0.24 & -3.68 \end{bmatrix}$$

### 6 Proposed algorithm (IEFHAC)

The use of the smart healthcare system in smart cities is increasing exponentially as it provides timely access to the patient records that not only provide on-time treatment

to the patient but also keeps the doctor out of patients' contact in critical present pandemic-like situations. However, the use of the internet for such important records can cause risk to the data that needs to be secure during transmission. Keeping this in view, the proposed IEFHAC framework has been presented. The proposed IEFHAC technique can be represented by a block diagram which is shown in Fig. 6. For confusion, pixel permutation is done with the help of Random Sequence Generation (RSG) using two chaotic maps i.e., Logistic chaotic map and Sine chaotic map already discussed in section 4. The output for one iteration of the one map is the initial value for the second map, and the first iteration value of the second map is further used as the initial value of the first map, so on and so forth [refer to Fig. 7]. In this way, the outputs of the overall iterations for both maps are different and hence balance key length requirement as compared to the single map or the double maps, as the initial value is set once, while in the proposed method the initial value itself goes on varying. The generated chaotic sequence is then XORed with the pixels of an image and hence creates more confusion among the pixels. The process of confusion is shown in Algorithm 1.

The bifurcation plot for the proposed random sequence with the chaotic maps is shown in Fig. 8. From the diagram, one can see that the presented method shows the more behavioral change in the system with a change in the parametric value. Further, the Lyapunov exponent of the proposed way is presented in Fig. 9 that shows the system is more sensitive to initial conditions.

In the process of diffusion, pixel values of the confused image are modified with the Hessenberg transformation described in section 5. The confused image (CI) is transformed twice with the Hessenberg principle, once directly and secondly by doing rotation or transpose before and after the processing of the confused image shown in

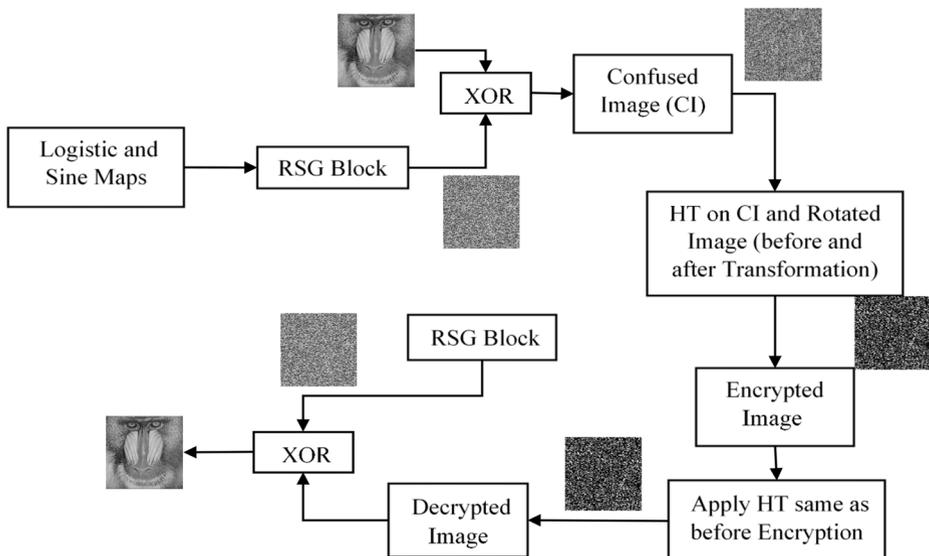


Fig. 6 Block Diagram of the Proposed IEFHAC Algorithm

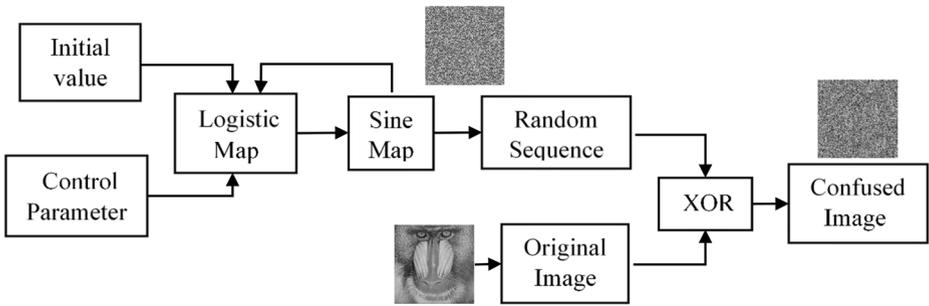


Fig. 7 Block Diagram for Confusion Process

Fig. 10. Then, the XOR operation is performed between these two transformed images. Algorithm II describes the diffusion process with the Hessenberg transformation.

**Algorithm I:** Confusion Process

**Input:** Original image ‘ $I_{(m,n)}$ ’, Two chaotic maps with the initial value of only one map and the only control parameter of other maps.

**Output:** Confused image ‘ $C_{(m,n)}$ ’.

**BEGIN**

- 1:  $r \leftarrow$  control parameter for Logistic map
- 2:  $x_n \leftarrow$  initial condition for Logistic map
- 3:  $u \leftarrow$  control parameter for Sine map
- 4: **for** rounds  $\leftarrow 1: m \times n - 1$
- 5:     **If** round  $\leftarrow 1$  **do**
- 6:          $x_{n+1} = r x_n (1 - x_n)$ .
- 7:         **else do**
- 8:              $x_{n+1} = r y_{n+1} (1 - y_{n+1})$ .
- 9:              $y_{n+1} = u \sin (\pi x_{n+1})$ .
- 10:         **end if**
- 11:     **end for**
- 12:  $Y \leftarrow$  reshape  $y_{(1, m \times n)}$  to  $y_{(m, n)}$
- 13:  $C \leftarrow I \otimes Y$

**End Algorithm I**

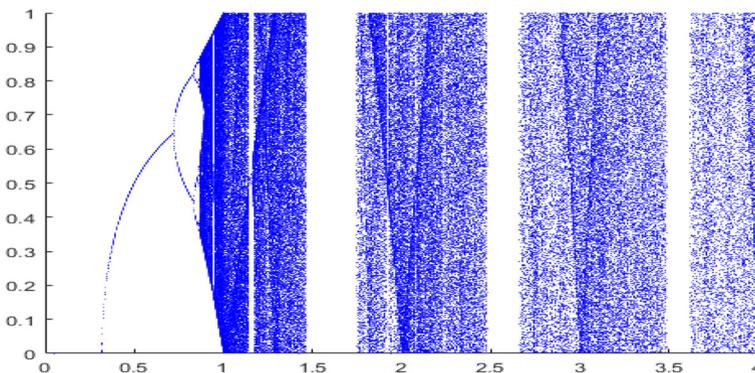


Fig. 8 Bifurcation Plot for Generated Random Sequence

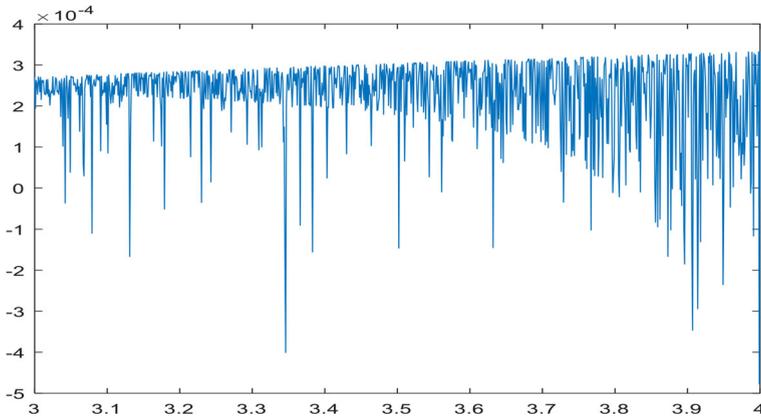


Fig. 9 Lyapunov Exponent for Generated Random Sequence

**Algorithm II:** Diffusion Process

**Input:** Confused image ‘ $C_{(m,n)}$ ’, Symmetric matrix, and Identity matrix for finding household matrix.

**Output:** Encrypted image ‘ $E_{(m,n)}$ ’.

**BEGIN**

- 1:  $C_r \leftarrow 180^\circ$  Rotated image
- 2:  $U \leftarrow$  household (orthogonal) matrix
- 3:  $U' \leftarrow$  Transpose (Inverse) of  $U$
- 4: **for** rounds  $\leftarrow 1: m \times n - 1$
- 5:      $H1 = U' \times C_r \times U$
- 6:      $HI \leftarrow 180^\circ$  Rotated  $H1$  image
- 7:      $H = U' \times C \times U$
- 8: **end for**
- 9:  $E = H \otimes HI$

**End Algorithm II**

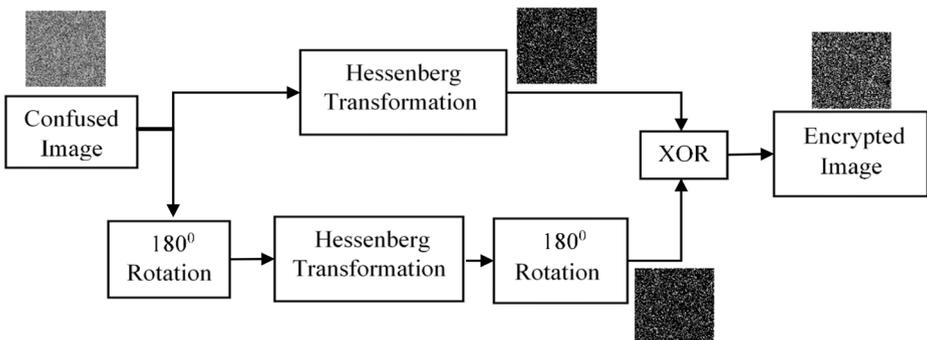


Fig. 10 Diffusion Process Block Diagram

## 6.1 Encryption process

This section includes the prologue for the computation of the encryption process in which the initial values are set once for the single map and for the rest one it is generated by itself. The encryption process of the proposed method is described in Algorithm III.

---

### Algorithm III: Encryption Process

---

**Input:** Original image 'I<sub>(m,n)</sub>', Keys 'r, x<sub>0</sub>, u', and household matrix 'U'.

**Output:** Encrypted image 'E<sub>(m,n)</sub>'.

---

**BEGIN**

- 1:  $C_r \leftarrow$  180° Rotated image
- 2:  $U' \leftarrow$  Transpose (Inverse) of U
- 3:  $Y \leftarrow$  Random sequence generated using two maps
- 4: **for** rounds  $\leftarrow$  1:  $m \times n - 1$
- 5:      $C = I \otimes Y$
- 6:     **for** rounds  $\leftarrow$  1:  $m \times n - 1$
- 7:          $H1 = U' \times C_r \times U$
- 8:          $HI \leftarrow$  180° Rotated H1 image
- 9:          $H = U' \times C \times U$
- 10:     **end for**
- 11: **end for**
- 12:  $E = H \otimes HI$

**End Algorithm III**

---

The encryption process of the proposed method is also applicable to color images, the only difference is that the image is separated into three planes and the method of encryption is processed on each plane individually. And the encrypted planes are concatenated to form the final encrypted image.

The following algorithm along with Fig. 11 explains the confusion and diffusion process. The detailed process is explained as follows:

1. To confuse image pixels both Logistic and Sine maps need two initial values ( $V_i = 1, 2, 3, 4$ ) to generate a random sequence ( $S_n = 1, 2, \dots, n$ ).
2. At first, two initial values ( $V_1, V_2$ ) for the first map (Logistic map, Eq. 1) are given directly to generate the first sequence value ( $S_1$ ).
3. For the next two initial values ( $V_3, V_4$ ) of a second map (Sine map, Eq. 2), one value is the previously generated sequence value ( $V_3 = S_1$ ) and the other initial value ( $V_4$ ) is given directly to generate the second sequence value ( $S_2$ ).
4. For the generation of third sequence value ( $S_3$ ), the first map (Logistic map, Eq. 1) uses one value ( $V_1 = S_2$ ) as previously generated value ( $S_2$ ) from a second map (Sine map), and another initial value ( $V_2$ ) directly and so on.
5. Generated chaotic sequence is converted into matrix form to XOR it with Image matrix for confused image formation.
6. Resultant confused image is transformed with the Hessenberg principle (Explained in Example 1 of section 5) as shown in Fig. 10 to form an encrypted image.

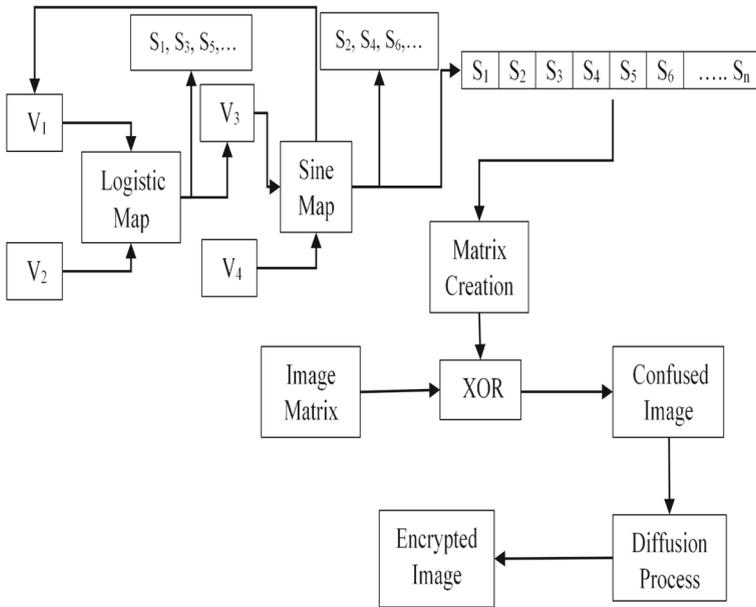


Fig. 11 Example of Encryption Process

### 6.2 Decryption process

This section masquerades the decryption process. The encrypted image formed after confusion and diffusion process can be decrypted back to acquire the original image. The decryption process for recovering back the original image is the reverse of the encryption process that is shown in Algorithm IV.

---

#### Algorithm IV: Decryption Process

---

**Input:** Encrypted image ‘ $E_{(m,n)}$ ’, Keys ‘ $r, x_0, u$ ’, and household matrix ‘ $U$ ’.

**Output:** Original image ‘ $I_{(m,n)}$ ’.

---

```

BEGIN
1:  $E_r \leftarrow 180^0$  Rotated image
2:  $U' \leftarrow$  Transpose (Inverse) of  $U$ 
3:  $Y \leftarrow$  Random sequence generated using two maps
4: for rounds  $\leftarrow 1: m \times n - 1$ 
5:    $H2 = U' \times E_r \times U$ 
6:    $HI2 \leftarrow 180^0$  Rotated  $H2$  image
7:    $H2 = U' \times E \times U$ 
8:    $C = H2 \otimes HI2$ 
9:   for rounds  $\leftarrow 1: m \times n - 1$ 
10:     $I = C \otimes Y$ 
11:   end for
12: end for
End Algorithm IV

```

---

The decryption process for color images is the reverse step of the encryption method.

## 7 Simulation results and discussions

IEFHAC has been tested on various images (Medical as well as general images) taken from the University of Southern California – Signal and Image Processing Institute (UPC-SIPI), Uncompressed Color Image Database (UCID), and Open Access Biomedical Image (OPENi) databases. However, the Covid-19 patient’s medical image has been taken from the GITHUB image dataset [9]. Because of the space limitations, analysis of randomly chosen nine images each size  $256 \times 256$  is displayed, shown in Fig. 12. The technique is applicable to both gray images as well as color images of different image sizes with different formats. Since the encryption and decryption of color images are the same as gray-scale images, therefore, the scheme is evaluated only on test gray-scale images (refer to Fig. 12). However, to show the applicability of the proposed method to the color images as well, the NPCR and UACI values are given for both grayscale images and color images given in section 7.2. Encryption of the image is performed with initial conditions shown in Table 1.

In this section, we present the experimental results of the proposed technique to evaluate the system for security and computational complexity. The scheme has been evaluated in terms of

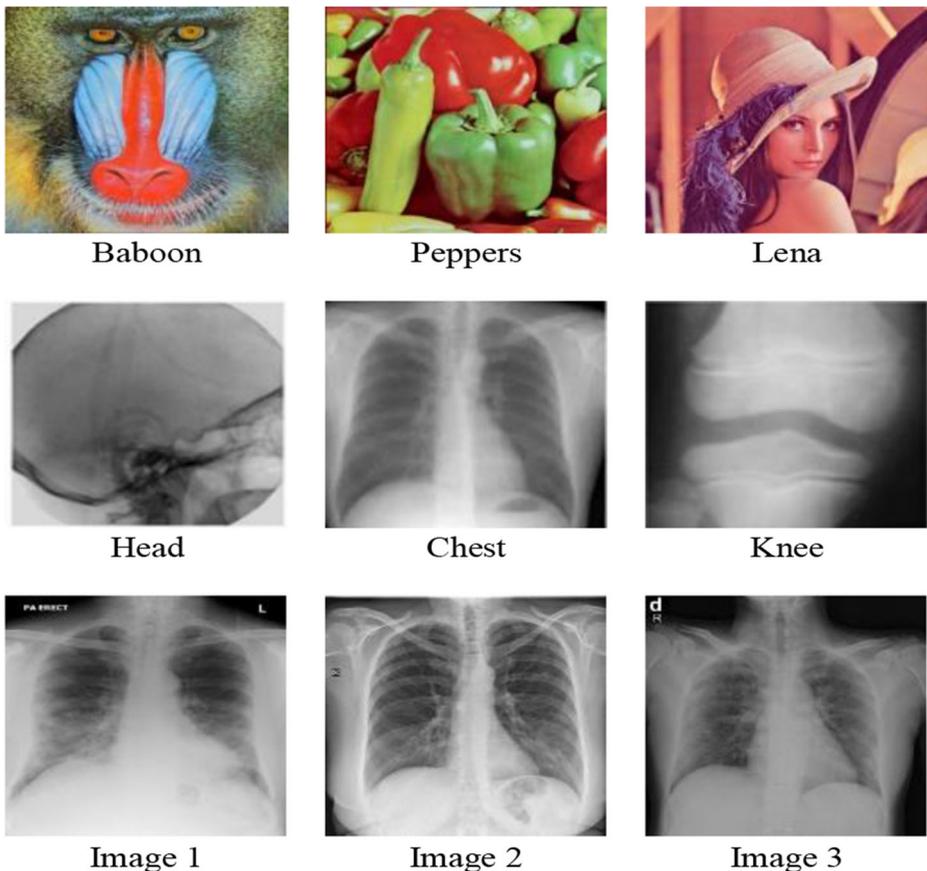


Fig. 12 General Images used for Encryption

**Table 1** Initial Values used for the Proposed Algorithm

Maps	Parameters		
	$x_0$	$r$	$\mu$
Logistic map	0.90	3.5	–
Sine map	first iteration output	–	0.99

the histogram, the Number of Pixels Change Rate (NPCR), Unified Average Change Intensity (UACI), computational time, etc.

## 7.1 Histogram analysis

Histogram analysis displays the pixel's intensity distribution of the digital image. An encrypted image should have a uniform distribution. When an image shows random behavior, i.e., it has a uniform distribution, then it is difficult for an anonymous adversary to attack or modify the secret information. The histograms of the plain images and resultant encrypted images, using the proposed scheme are shown in Fig. 13. It can be seen that encrypted image histogram show uniformity among different pixels, indicating that the proposed algorithm is robust and can prevent leakage of secret information from any statistical attacks. The histogram analysis has been also done on a number of images randomly chosen from UPC-SIPI and the result shows a similar/ nearly uniform behavior as that of the images displayed.

To test the uniformity of histogram, a chi-square test has been used which is computed by the following equation [46].

$$\chi^2 = \sum_{d=0}^{255} \frac{(f_d - s)^2}{s} \quad (10)$$

Where  $f_d$  is the pixel value frequency (0–255),  $s = (r \times c)/256$  is the size of an image in which  $r$  and  $c$  are the image dimensions. The lower chi-square value represents better uniformity. The Chi-square value of the above-shown histogram for different gray images is reported in Table 2. The analyzed test confirms the histogram uniformity of the stated encrypted images.

## 7.2 Differential analysis

Differential analysis checks the sensitivity of the encrypted image to its original image and secret key. The strength of the encrypted image has been checked with the two well-known standard criteria: NPCR and UACI tests. NPCR checks the pixel modification in an original image with the encrypted image. It estimates the sensitivity of the encrypted image about its original image and initial values/parameters. The NPCR is described in Eq. 11 where  $m \times n$  is the image size. Here,  $D$  is the number of uneven values that can be found with Eq. 12 in which  $I_0$  is the original image and  $I_e$  is the encrypted image.

$$NPCR = \frac{1}{mn} \sum_{i,j=1}^{mn} D(i,j) \times 100\% \quad (11)$$

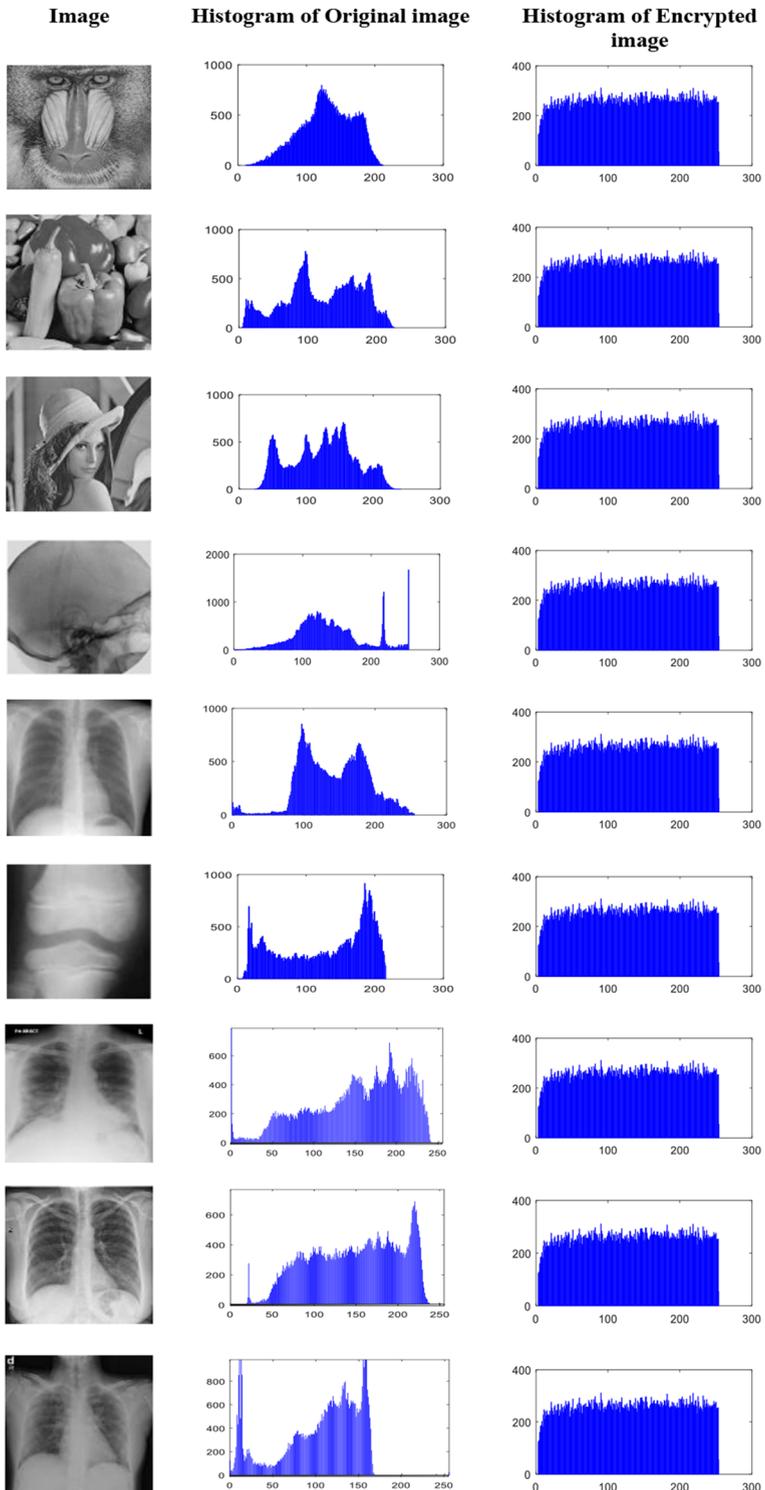


Fig. 13 Histogram of Original and Encrypted Image for General and Medical Images

$$D = \begin{cases} 0, & \text{if } I_0 = I_e \\ 1, & \text{if } I_0 \neq I_e \end{cases} \quad (12)$$

UACI is the average intensity change between the original image and the encrypted image. UACI test can be evaluated with Eq. 13. Here,  $I_0$  and  $I_e$  are the original and encrypted images with  $m \times n$  dimensions.

$$UACI = \frac{1}{mn} \left( \sum_{i,j=1}^{mn} \frac{|I_0(i,j) - e(i,j)|}{255} \right) \times 100\% \quad (13)$$

As per [16] for a secure cryptosystem, NPCR and UACI should be near 99.61% and 33.44% respectively. The evaluation values for gray-scale and color test images are shown in Tables 3 and 4 and its comparison with the existing techniques for NPCR and UACI are given in Table 5. To make the analysis precise, the study has considered six images from Fig. 12 for color image encryption analysis. The calculated examinations show that the proposed algorithm has better sensitivity values than the existing state-of-the-art algorithms. Additionally, the proposed technique has been also tested on various medical images randomly taken from the OPENi medical image repository, in which the average NPCR is near about 99.76%, and UACI value is 36.52%, that shows the excellence of the scheme.

### 7.3 Keyspace analysis

The number of keys that can be used in the encrypted technique is the keyspace of the algorithm. IEFHAC uses two chaotic maps having two keys each. Total combinations of different keys that can be used are  $10^{42}$  if the average precision set is  $10^{-14}$ , which means the proposed scheme guarantees to withstand any brute-force attack.

**Table 2**  $\chi^2$  values of Fig. 13 for different gray-scale images

Image	$\chi^2$	Outcome
Baboon	98,566	
Encrypted-Baboon	268	Uniform
Peppers	31,701	
Encrypted- Peppers	250	Uniform
Lena	41,248	
Encrypted-Lena	248	Uniform
Head	63,137	
Encrypted-Head	257	Uniform
Chest	53,122	
Encrypted-Chest	255	Uniform
Knee	38,177	
Encrypted-Knee	252	Uniform
Image 1	34,370	
Encrypted-Image 1	251	Uniform
Image 2	29,134	
Encrypted-Image 2	247	Uniform
Image 3	89,636	
Encrypted-Image 3	266	Uniform
<b>Average (Encrypted)</b>	<b>253.23</b>	<b>Uniform</b>

**Table 3** NPCR and UACI Values for different gray-scale images

Images	NPCR	UACI
Baboon	99.7849	36.1264
Peppers	99.7101	34.4092
Lena	99.7070	34.7772
Head	99.7635	38.5166
Chest	99.7574	40.3556
Knee	99.7391	37.8921
Image 1	99.1974	43.8738
Image 2	99.8230	42.6622
Image 3	99.6506	30.5751
Average	<b>99.6815</b>	<b>37.6876</b>

### 7.4 Key sensitivity analysis

Key sensitivity refers to a one-bit change in the key that leads to altogether different results. Wrong key substitution in the algorithm results in an incorrect decrypted image. The general and medical test images have been used to test the sensitivity of the key for which the image is decrypted with a wrong key (bit change in a logistic key: from 0.90 to 0.91) and the effects of only nine images are displayed, shown in Fig. 14. From the diagram, it can be observed that the decrypted image is different and wrong in comparison to the original one that shows the high sensitivity of the proposed algorithm.

### 7.5 Computational time analysis

Computational time determines the time a system takes to complete the process of encryption/decryption that is helpful to check the system's efficiency. This analysis is carried out on an Intel®, Core™ i3-3120M, CPU @ 2.50GHz, 4 GB RAM running Windows 10. Simulation results for time analysis for encryption and decryption are shown in Table 6. The time required to encrypt an image is the encryption time, whereas, decryption time is the image decryption processing time. For encryption, too many processing steps are required to complete the task while as in decryption, the method uses generated random sequence directly which has already been generated in the encryption process instead of generating it again, as the sequence will be the same either processing it once or twice. Hence, the encryption processing time is more than the decryption computation time. Time taken to complete the encryption/decryption process can be calculated by dividing the size of data by the speed shown in Eq. 14. It is clear from the table that the proposed technique takes less time for encryption and decryption and hence is less complex in terms of speed.

**Table 4** NPCR and UACI Values for different color images

Images	NPCR	UACI
Baboon	99.7447	35.2758
Peppers	99.0560	33.7358
Lena	99.7375	36.7183
Head	99.7986	38.5553
Chest	99.7482	40.2695
Knee	99.7116	37.9899
Average	<b>99.6327</b>	<b>37.0907</b>

**Table 5** Comparison of NPCR and UACI Values

Algorithm	NPCR	UACI
Anwar et al. [2]	98.74	–
Ayoub et al. [3]	99.63	27.76
Patro et al. [39]	99.61	33.41
Parah et al. [36]	99.01	34.82
Ghebleh et al. [13]	99.56	33.70
Ye et al. [53]	99.62	33.51
Tsafack et al. [46]	99.61	33.53
Hamza et al. [28]	99.61	33.61
Njitacke et al. [34]	99.63	–
Tsafack et al. [47]	99.63	33.53
Proposed	<b>99.66</b>	<b>37.39</b>

$$Time = \frac{Data\ size}{speed} \quad (14)$$

Where,  $Data\ size = \frac{cycles}{second}$  and  $Speed = \frac{cycles}{byte}$

## 7.6 Randomness analysis

The randomness experiment for the proposed algorithm has been tried with the NIST statistical test suite (SP 800–22) [8]. This test suite includes almost 15 computable tests. The results for these tests for IEFHAC are shown in Table 7.

The proposed algorithm has passed all the tests that show the randomness of the scheme.

## 7.7 Decrypted image quality analysis

To evaluate the quality of a decrypted image, various image quality analysis has been used. The investigation includes the Structural Similarity Index (SSIM), Normalized Cross-Correlation (NCC), and Bit Error Rate (BER). SSIM checks the likeness between the original image and the decrypted image. It can be calculated with Eq. 15 [14], where  $\mu$  represents the intensity of an image,  $\sigma$  represents the standard deviation, and  $\sigma$  of  $(x, y)$  represents the cross-correlation of an image. NCC checks the relation between the original and decrypted image. It can be calculated through Eq. 16 [14] in which  $w_o$  and  $w_x$  are the original and encrypted image bits. The decrypted image should have SSIM and NCC values close or equal to 1 which means the image is decrypted perfectly. BER represents the error between the original image and the encrypted image. Here, the BER should be near or equal to 0 which indicates the image is decrypted without any error. The mathematical representation of BER [42] is shown in Eq. 17 wherein  $N_{err}$  and  $N_{bits}$  symbolize the number of error bits and the number of pixels respectively.

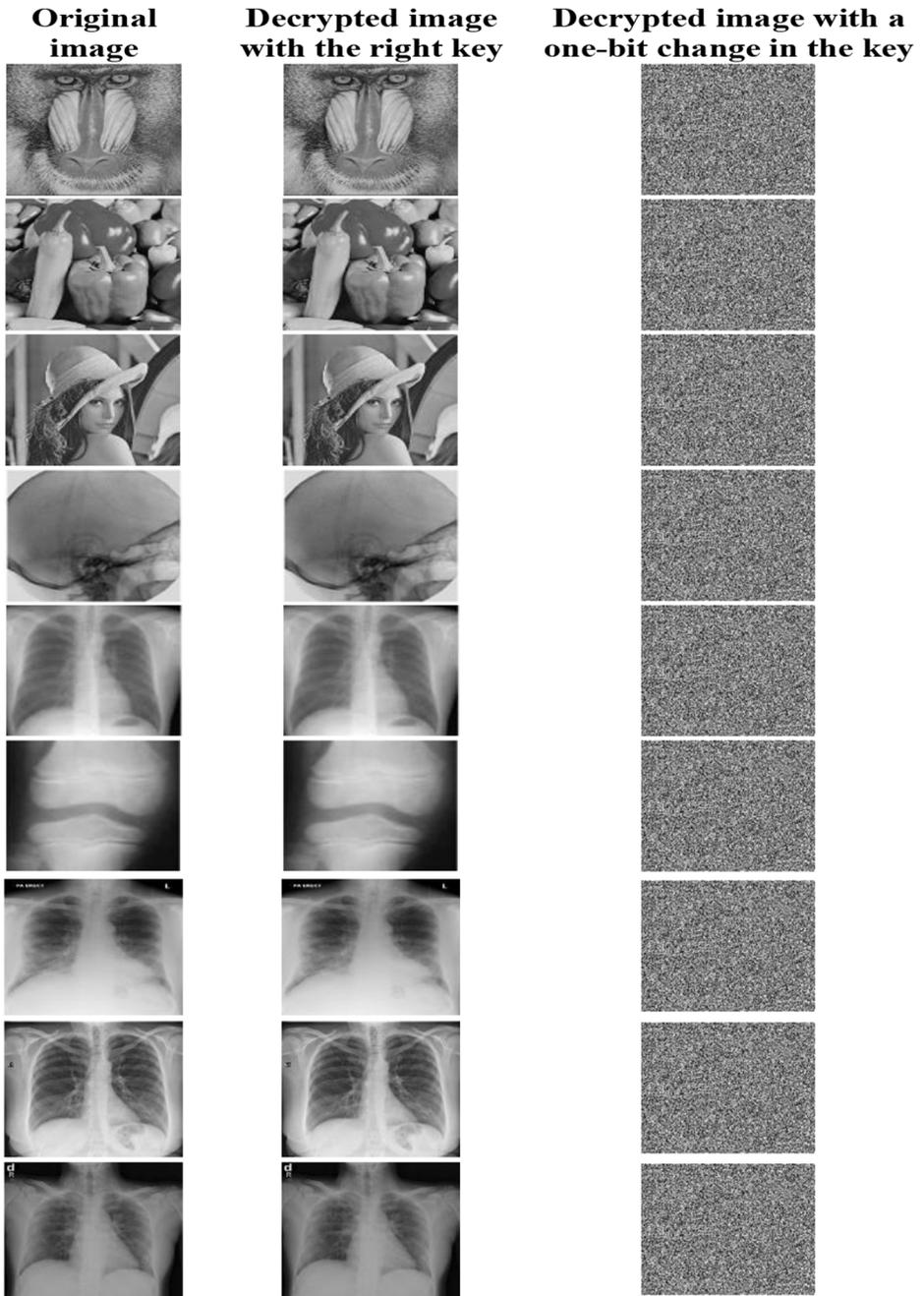


Fig. 14 Key Sensitivity test: Decryption with Original and Wrong Key

**Table 6** Computation Time Comparison with the Existing Techniques

Algorithm	Encryption time (s)	Decryption time (s)
Ayoub et al. [3]	7.37	–
Patro et al. [39]	1.78	–
Hamza et al. [14]	0.95	0.96
Njitacke et al. [34]	0.21	–
Proposed	<b>0.34</b>	<b>0.02</b>

$$SSIM(x, y) = \frac{(2\mu_x\mu_y + C_1)(2\sigma_{xy} + C_2)}{(\mu_x^2 + \mu_y^2 + C_1)(\sigma_x^2 + \sigma_y^2 + C_2)} \quad (15)$$

$$NCC = \frac{\sum_{i=1}^m \sum_{j=1}^n w_o(i, j)w_x(i, j)}{\sum_{i=1}^m \sum_{j=1}^n [w_o(i, j)]^2} \quad (16)$$

$$BER = \frac{N_{err}}{N_{bits}} \quad (17)$$

The average estimated and comparison values of these quality analysis tests for a number of images randomly selected from the USC-SIPI image database are shown in Table 8.

**Table 7** NIST Statistical tests

Statistical test	Decision
Frequency test	Passed
Frequency within a block test (Block sizes: 3, 4, 5, 6, 7, 8)	Passed
The runs test	Passed
Tests for the longest run of ones in a block (Block size:8)	Passed
The binary matrix rank test (4 Matrices, Rows 8, Columns 8)	Passed
The discrete Fourier transform test	Passed
The non-overlapping template matching test (Template length=4, Blocks=2, 4, 8)	Passed
The overlapping template matching test (Template length=4, Blocks=4, 8)	Passed
Maurer's universal statistical test	Passed
The approximate entropy test	Passed
The cumulative sums test	Passed

**Table 8** Image Quality Value Results Between Original and Decrypted Image

Algorithm	SSIM	NCC	BER
Hamza et al. [14]	0.9994	1	–
Proposed	1.0000	1	0

## 8 Conclusion

Smart health systems are distinguished by the use of Information and Communication Technology (ICT) in healthcare. The implementation of technology-based solutions in healthcare can lead to better diagnosis and treatment of diseases. This will bring about an overall improvement in the quality of care provided to the patients. In smart e-health systems, the security of medical images plays an instrumental role in proper service delivery. Image data security has become a major concern to mitigate the confidentiality issues related to sensitive medical data during transmission in critical situations. Ensuring the security of medical images is imperative for the efficient implementation of Smart health infrastructures. In this paper, we present IEFHAC, a secure and less computationally complex image encryption technique based on two chaotic maps and Hessenberg household transformation. The algorithm comprises two stages: the confusion stage and the diffusion stage. The confusion stage randomizes the image using a Logistic map and Sine map, whereas, the diffusion stage transforms the confused-image with the help of the Hessenberg principle. The chaotic sequence generation method makes the system strong against attacks and it is difficult for the anonymous person to find the exact key for decryption because one of the keys itself is random. Furthermore, the Hessenberg principle transforms the confused-image with altogether different pixel values that add more security to the system. The scheme shows better performance in terms of security as well as time and can withstand many attacks, like, differential attacks, statistical attacks, etc. IEFHAC shows better results than the already existing algorithms in terms of NPCR, UACI, and computational time with 99.66% - 100%, 37.39%, and 0.36 s respectively. Thus, IEFHAC could be used for real-life medical applications in smart healthy cities.

## References

- 2020 Breach Barometer: 41Mpatient Records Breached as hacking incidents escalate.(2020), <https://blog.protenus.com/2020-breach-barometer-41m-patient-records-breached-as-hacking-incidents-escalate> (9-12-2010)
- Anwar S, Meghana S (2019) A pixel permutation based image encryption technique using chaotic map. Springer Multimedia Tools Appl 78:27569–27590. <https://doi.org/10.1007/s11042-019-07852-2>
- Ayoub AM, Hussein AH, Attia MAA (2016) Efficient selective image encryption. Springer Multimedia Tools Appl 75:17171–17186. <https://doi.org/10.1007/s11042-015-2985-7>
- Bibri SE, Krogstie J (2017) Smart sustainable cities of the future: an extensive interdisciplinary literature review. Sustain Cities Soc 31:183–212
- Cao SJ, Ding J, Ren C (2020) Sensor deployment strategy using cluster analysis of fuzzy C-means algorithm: towards online control of indoor Environment's safety and health. Elsevier Sustain Cities Soc 59:102190. <https://doi.org/10.1016/j.scs.2020.102190>
- Chan EYS, Corless RM, Gonzalez-Veg L, Sendra JR, Sendra J, Thornton SE (2020) Upper Hessenberg and Toeplitz Bohemians. Elsevier Linear Algebra Appl 601:72–100. <https://doi.org/10.1016/j.la.2020.03.037>
- Chen JX, Zhu ZL, Fu C, Zhang LB, Zhang Y (2015) An image encryption scheme using nonlinear inter-pixel computing and swapping based permutation approach, Commun. Nonlinear Sci Numer Simul 23(1): 294–310

8. Cicek I, Pusane AE, Dundar G (2017) An integrated dual entropy Core true random number generator. *IEEE Trans Circ-II* 64:329–333
9. Covid-19 patients image dataset is available on: <https://github.com/education454/datasets/tree/master/Data>
10. Data Breaches. Orion Sang reports data loss of patients (2020). URL <https://www.databreaches.net/oakland-county-stops-covid-19-data-leak/> (17-04-2020).
11. Data Breaches. Dimitris Koumitsidis reports data loss of patients including a politician (2020). URL <https://www.databreaches.net/teenage-hacker-arrested-in-madrid-for-hacking-medical-data-and-leaking-information-on-a-politician-positive-for-covid-19/> (18-04-2020).
12. Dogan S (2017) A data hiding scheme based on chaotic map and pixel pairs. *J Digital Forensics Secur Law* 12(4). <https://doi.org/10.15394/jdfsl.2017.1456>
13. Ghebleh M, Kanso A, Stevanović D (2018) A novel image encryption algorithm based on piecewise linear chaotic maps and least squares approximation, *Springer Multimedia Tools Appl* 77:7305–7326. <https://doi.org/10.1007/s11042-017-4634-9>.
14. Hamza R, Yan Z, Muhammad K, Bellavista P (2019) A privacy-preserving cryptosystem for IOT e-healthcare. *Elsevier Inform Sci*. <https://doi.org/10.1016/j.ins.2019.01.070>
15. He J, Ying Q, Qian Z, Feng G, Zhang X (2020) Semi-structured data protection scheme based on robust watermarking. *Springer EURASIP J Image Video Processing* 2020. <https://doi.org/10.1186/s13640-020-00500-y>
16. Hu Z, Zhou Y (2016) Image encryption using 2D logistic-adjusted-sine map. *Inf Sci* 339:237–253
17. Hua Z, Jin F, Xu B, Huang H (2018) 2D logistic-sine-coupling map for image encryption. *Elsevier Signal Process* 149:148–161
18. Hussain I, Anees A, Aslam M, Ahmed R, Siddiqui N (2018) A noise resistant symmetric key cryptosystem based on S8 S-boxes and chaotic maps. *Eur Phys J Plus* 133(167). <https://doi.org/10.1140/epjp/i2018-11987-x>
19. Jiao S, Zou W, Li X (2017) QR code noise-free optical encryption and decryption of a gray scale image. *Elsevier Optics Commun* 387:235–240. <https://doi.org/10.1016/j.optcom.2016.11.066>
20. Jin J, Sun W, Al-Turjman F, Bilal K, Xiaodong Y (2020) Activity pattern Mining for Healthcare. *IEEE Access* 8:56730–56738. <https://doi.org/10.1109/ACCESS.2020.2981670>
21. Kaushik N, Sheokand K (2016) A steganography technique based on chaotic LSB and DWT. *Int J Innov Res Comput Commun Eng* 4(6):10420–10426. <https://doi.org/10.15680/IJIRCC.2016.0406028>
22. Ke G, Wang H, Zhou S, Zhang H (2019) Encryption of medical image with most significant bit and high capacity in piecewise linear Chaos graphics. *Elsevier Measurement* 135:385–391. <https://doi.org/10.1016/j.measurement.2018.11.074>
23. Khan FA, Asif M, Ahmad A, Alharbi M, Aljuaid H (2020) Blockchain technology, improvement suggestions, security challenges on the smart grid and its application in healthcare for sustainable development. *Sustain Cities Soc* 55:102018 ISSN 2210-6707
24. Kumar RR, Jayasudha S, Pradeep S (2016) Efficient and secure data hiding in encrypted images: a new approach using Chaos. *Taylor & Francis Inform Security J: Global Perspective* 25(4–6):235–246. <https://doi.org/10.1080/19393555.2016.1248582>
25. Kumari M, Gupta S, Sardana P (2017) A survey of image encryption algorithms, *springer 3D. Research* 8(37)
26. Laufs J, Borrión H, Bradford B (2020) Security and the Smart City: a systematic review. *Sustain Cities Soc* 55:102023
27. Li C, Feng B, Li S, Kurths J, Chen G (2019) Dynamic analysis of digital chaotic maps via state-mapping networks. *IEEE Trans Circ Systems-I: Regular Papers* 66(6):2322–2335. <https://doi.org/10.1109/TCSI.2018.2888688>
28. Liao X, Li K, Yin J (2017) Separable data hiding in encryption image based on compressive sensing and discrete Fourier transform. *Springer Multimedia Tools Appl*. <https://doi.org/10.1007/s11042-016-3971-4>
29. Lin Z, Liu J, Lian J, Ma Y, Zhang X (2019) A novel fast image encryption algorithm for embedded systems. *Springer Multimedia Tools Appl* 78:20511–20531. <https://doi.org/10.1007/s11042-018-6824-5>
30. Loan NA, Hurrah NN, Parah SA, Lee JW, Sheikh JA, Bhat GM (2018) Secure and robust digital image watermarking using coefficient differencing and chaotic encryption. *IEEE Trans Inform Secur Solut Telem Appl* 6:19876–19897. <https://doi.org/10.1109/ACCESS.2018.2808172>
31. Luo Y, Yu J, Lai W, Liu L (2019) A novel chaotic image encryption algorithm based on improved baker map and logistic map. *Springer Multimedia Tools Appl* 78:2023–22043. <https://doi.org/10.1007/s11042-019-7453-3>
32. Lyche T (2020) Numerical Eigenvalue Problems. *Springer Cham Numerical Linear Algebra Matrix Factorizations, Comput Sci Eng* 22:317–334. [https://doi.org/10.1007/978-3-030-36468-7\\_14](https://doi.org/10.1007/978-3-030-36468-7_14)
33. Merchant F, Vatwani T, Chatopadhyay A, Raha S, Nandy SK (2018) Efficient Reliaization of Household Transform Through Algorithm-Architecture Co-Design for Acceleration of QR Factorization *IEEE Transaction on Parallel and Distribution Systems* 29(8):1707–1720.

34. Njitacke ZT, Isaac SD, Nestor T, Kengne J (2020) Window of multistability and control in a simple 3D Hopfield neural network: application to biomedical image encryption. *Springer Neural Comput Appl*:1–20. <https://doi.org/10.1007/s00521-020-05451-z>
35. Pak C, Huang L (2017) A new color image encryption using combination of the 1D chaotic map. *Elsevier Signal Processing* 138:129–137. <https://doi.org/10.1016/j.sigpro.2017.03.011>
36. Parah SA, Loan NA, Shah AA, Sheikh JA, Bhat GM (2018) A new secure and robust watermarking technique based on logistic map and modification of DC coefficients. *Springer Nonlinear Dynam* 93:1933–1951. <https://doi.org/10.1007/s11071-018-4299-6>
37. Parvin Z, Seyedarabi H, Shamsi M (2016) A new secure and sensitive image encryption scheme based on new substitution with chaotic function. *Springer Multimedia Tools Appl* 75:10631–10648. <https://doi.org/10.1007/s11042-014-2115-y>
38. Patro KAK, Acharya B (2020) A novel multi-dimensional multiple image encryption technique. *Springer Multimedia Tools Appl* 79:12959–12994. <https://doi.org/10.1007/s11042-019-08470-8>
39. Patro KAK, Acharya B (2020) A novel multi-dimensional multiple image encryption technique. *Springer Multimedia Tools Appl* 79:12959–12994. <https://doi.org/10.1007/s11042-019-08470-8>
40. Ping P, Fan J, Mao Y, Xu F, Gao Z (2019) a Chaos-based image encryption scheme using digit-level permutation and block diffusion, *IEEE transaction article in press*.
41. Prasad S, Pal AK (2019) Logistic map-based image steganography scheme using combined LSB and PVD for security enhancement. *Springer Emerging Technologies in Data Mining/Inform Security Advances Intell Syst Comput*. [https://doi.org/10.1007/978-981-13-1501-5\\_17](https://doi.org/10.1007/978-981-13-1501-5_17)
42. Saidi M, Hermassi H, Rhouma R, Belghith S (2017) A new adaptive image steganography based on DCT and chaotic map. *Springer Multimedia Tools and Appl* 76:13493–13510. <https://doi.org/10.1007/s11042-016-3722-6>
43. Sankpal PR, Vijaya PA (2014) Image encryption using chaotic maps: a survey, *Fifth International Conference on Signals and Image Processing*.
44. Silva BN, Khan M, Han K (2018) Towards sustainable smart cities: a review of trends, Architectures, Components, and Open Challenges in Smart Cities. *Sustainable Cities Soc* 38:697–713
45. Su Q, Wang G, Lv G, Zhang X, Deng G, Chen B (2016) A novel blind color image watermarking based on Contourlet transform and Hessenberg decomposition. 76:8781–8801. <https://doi.org/10.1007/s11042-016-3522-z>
46. Tsafack N, Kengne J et al (2019) Design and development of a simple dynamical 4-D chaotic circuit with applications in image encryption. *Elsevier Inform Sci*. <https://doi.org/10.1016/j.ins.2019.10.070>
47. Tsafack N, Sankar S et al (2020) A new chaotic map with dynamic analysis and encryption application in internet of health things. *IEEE Special Section on Lightweight Secur Provence Int Health Things* 8:137731–137744. <https://doi.org/10.1109/ACCESS.2020.3010794>
48. Turjman FA (2019) Smart-city medium access for smart mobility applications in internet of things. *Wiley: Special Issue Article Trans Emerging Tel Tech*. <https://doi.org/10.1002/ett.3723>
49. Wu W, Yu Y, Luo Q, Yao D, Li Q, Chai X (2020) Calculation of higher Eigen-modes of the forward and Adjoint neutron diffusion equations using IRAM algorithm based on domain decomposition. *Ann Nucl Energy* 143:107463
50. [www.Covidvisualizer.com](http://www.Covidvisualizer.com), accessed on 17-01-2021.
51. Xu L, Li Z, Li J, Hua W (2016) A novel bit-level image encryption algorithm based on chaotic maps. *Opt Lasers Eng* 78:17–25
52. Yang J, Liao X (2020) An embedding strategy on fusing multiple image features for data hiding in multiple images. *Elsevier J Vis Commun Image R* 71:102822. <https://doi.org/10.1016/j.jvcir.2020.102822>
53. Ye G, Huang X (2018) Spatial image encryption algorithm based on chaotic map and pixel frequency. *Sci China Inform Sci* 61:058104:1–058104. <https://doi.org/10.1007/s11432-017-9191-x>
54. Zhou L, Feng G, Shen L, Zhang X (2019) On security enhancement of steganography via generative adversarial image. *IEEE Trans Signal Process Lett*. <https://doi.org/10.1109/LSP.2019.2963180>
55. Zou N, Liang S, He D (2020) Issues and challenges of user and data interaction in healthcare-related IoT: a systematic review, *Emerald Library Hi-Tech*, ISSN: 0737-8831, <https://doi.org/10.1108/LHT-09-2019-0177>.