Big Data Research 25 (2021) 100225

Contents lists available at ScienceDirect

Big Data Research

www.elsevier.com/locate/bdr

A Security Management Framework for Big Data in Smart Healthcare

Parsa Sarosh [a], Shabir A. Parah [a,*], G. Mohiuddin Bhat [b], Khan Muhammad [c,*]

[a] Post Graduate Department of Electronics and Instrumentation Technology, University of Kashmir, Srinagar, India
[b] Department of Electronics and Communication Engineering, Institute of Technology, Zakoora, India
[c] Visual Analytics for Knowledge Laboratory, Department of Software, Sejong University, Seoul 143-747, Republic of Korea

ARTICLE INFO

Article history:
Received 21 September 2020
Received in revised form 3 February 2021
Accepted 13 March 2021
Available online 31 March 2021

Keywords:
Big Data
Telehealthcare
Data security
DNA encryption
Secret image sharing
Hyperchaotic system

ABSTRACT

Big Data analytics in the medical sector can assist medical professionals to facilitate improvement in healthcare. With the help of data analysis, clinical images of patients can be used to detect certain medical conditions. In the COVID-19 pandemic, many integrated technologies are being used to remodel the healthcare systems. The management of an integrated healthcare solution necessitates the need for security of the medical data. In this paper, we propose a security framework based on the Logistic equation, Hyperchaotic equation, and Deoxyribonucleic Acid (DNA) encoding. Subsequently, a Lossless Computational Secret Image Sharing (CSIS) method is used to convert the encrypted secret image into shares for distributed storage in cloud-based servers. Hyperchaotic and DNA encryption is performed to improve the overall security of the system. Furthermore, Pseudorandom Numbers (PRN) generated by the logistic equation are XORed with the image sequence in two phases by changing the parameters slightly. Finally, the application of Secret Sharing (SS) generates completely noise-like cipher images that enhance the security of the cloud-based cryptosystem. The generated shares are small in size and require fewer resources like storage capacity and transmission bandwidth which is highly desirable in IoT-based systems. It is verified that the cryptosystem is highly secure against attacks as well as interferences and has a very strong key-sensitivity.

1. Introduction

Internet of things (IoT) can facilitate digital health services during the COVID-19 pandemic by providing a healthcare management database for the patients, healthcare organizations, and government institutions [1,2]. Internet of Medical Things (IoMT) is a medical specific type of IoT that can facilitate digital health in the COVID-19 crisis. IoMT represents a network of sensors, communication, and computing devices that collect, process, and store the medical information. This information collected by the smart sensors along with the healthcare data like medical images, insurance, billing, and test reports is then sent to the cloud-based servers for processing, storage and, transmission [3]. Once the data is sent over to the IoT-based servers, the unencrypted data can be accessed and compromised by the adversaries. Cyber-attacks on IoT-based smart healthcare have increased tremendously in the last few years. In July 2019, around 8 and 12 million patient records were compromised from the LabCorp Clinical Laboratory and Quest Diagnostics, respectively. In December 2019, LifeLabs in Canada suffered a data breach that exposed around 15 million patient records. Furthermore, around 25 million records containing sensitive medical data were breached in 2019 incurring huge economic losses as reported by the Health IT security. Particularly, for the COVID-19 pandemic, the online consultation and Tele-diagnosis require the transfer and storage of clinical images over the IoT-based network [4]. However, without a proper security framework for the medical images, the sensitive data of the patients can be easily compromised [5,6]. This forms a major challenge in the management of the smart healthcare system. Medical images in the e-health database like a Personal Health Record (PHR) need to be completely secured before transmitting them to the IoT-based servers. This is shown in Fig. 1. Common security concerns namely manipulative usage, unauthorized access, and alteration of these clinical images need to be properly addressed. The above-mentioned motivating factors have led to the usage of techniques like encryption and steganography to ensure the security of medical images. However, to deal with issues of distributed storage, fault tolerance, reduction of secret data, and key management, the lossless CSIS has been introduced for securing images. The CSIS scheme generates small-sized shares for efficient transmission over the IoT-based network [7]. However, it suffers from the residual image problem which leads to leakage of information from

[*] Corresponding authors.
E-mail addresses: shabirparah@kashmiruniversity.ac.in, shabireltr@gmail.com (S.A. Parah), khan.muhammad.icp@gmail.com (K. Muhammad).

https://doi.org/10.1016/j.bdr.2021.100225

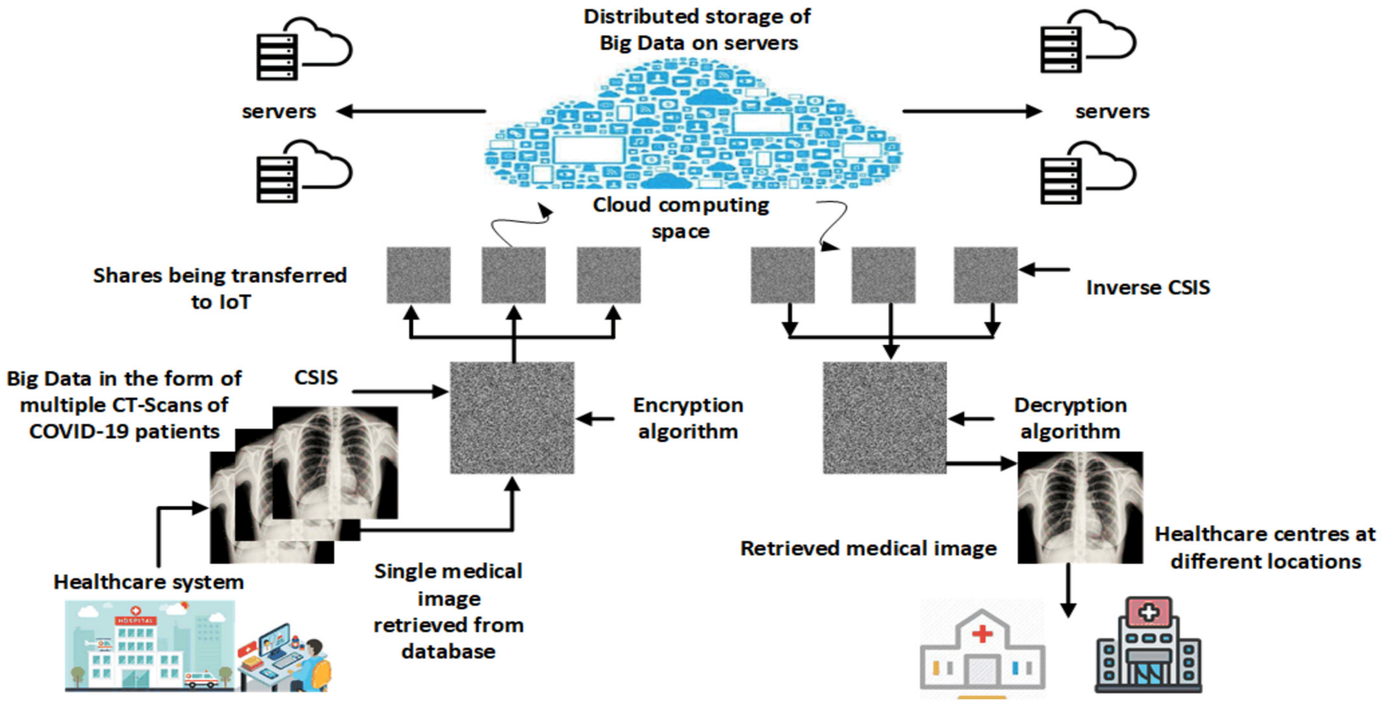


Fig. 1. Security solution for medical images in storage and transmission through the IoT-based smart healthcare for COVID-19 tele-diagnostics.

the secret shares. Application of encryption with CSIS can remove the residual image problem and can provide completely noise-like small-sized shares. Common encryption algorithms like Advanced Encryption Standard (AES) are not suitable for image encryption and consequently, many research works have been suggested to utilize the chaos-based cryptosystems for image encryption.

In this paper, we propose an advanced security framework based on the logistic equation, hyperchaotic equation, and DNA encoding. The medical images like the X-Ray and CT-Scans of COVID-19 patients are first encrypted using a hybrid chaos-based encryption technique. The hyperchaotic system is used to globally shuffle the image bits and the resulting sequence is further encrypted using the DNA encryption and logistic equation. Subsequently, the CSIS method is used to convert the encrypted secret image into shares for distributed storage in cloud-based servers [8]. When the image is to be accessed by another healthcare system, the threshold number of shares is utilized to recover the secret encrypted image by inverse CSIS. The image is then decrypted for further processing by the healthcare system. The received medical image is remotely analyzed to provide a proper diagnosis [9]. The clinical findings in the X-Ray and CT images like consolidation and crazy paving patterns can be indicative of the infection and degree of severity of the condition. This security framework ensures that the IoT-based healthcare system provides timely access to quality care by the reliable and secure transmission of medical data [10]. The need for security of medical images in the process of COVID-19 Telediagnosis has been described in detail in Section 3. The principal contributions of the proposed scheme are summarized as follows:

- The proposed scheme generates small-sized shares for distributed storage of medical images in the IoT-based servers.
- The residual image problem of CSIS is mitigated using an efficient chaos-based encryption algorithm. Our scheme generates completely noise-like share images that maintain the threshold property of the CSIS scheme.
- The use of DNA encryption along with a hybrid chaotic system further enhances the security strength of the algorithm.
- The proposed scheme can be used to secure both natural as well as medical images. It is best suited for an IoT-based smart healthcare system as it reduces the requirement of resources like storage space and transmission bandwidth. The share-data transmitted is less and the transmission time is also reduced.

The remainder of our paper is arranged as follows. Section 2 summarizes the review of relevant chaos-DNA-based algorithms and secret sharing algorithms as per the available literature. Section 3 illustrates the COVID-19 scenario and the need for IoT-based solutions. Section 4 discusses the 1-D chaotic system, hyperchaotic system, DNA encryption, and CSIS scheme. The proposed security model is presented in Section 5. Results and discussion are presented in Section 6. The conclusion of this research work is presented in Section 7.

2. Related work

Lossless CSIS has been proposed by Thien and Lin [11] and can be used for the distributed storage of medical images in IoT-based smart-health applications [12,13]. This is because a lossless CSIS scheme has many advantages like fault-tolerance, enhanced security, lossless reconstruction, and fast transmission of data [14,15]. However, the CSIS scheme has three main drawbacks, which are high computational complexity, residual image problem in shares, and more time required for secret reconstruction [16]. The residual image problem makes CSIS a ramp scheme, where the amount of information revealed is proportional to the number of shares involved in the secret reconstruction process [17]. This problem compromises the threshold nature of the scheme and also vitiates the security condition. As part of the original scheme proposed by Thien and Lin [18], the secret image is permuted to mitigate the residual image problem in shares. However, many research works have been directed to analyze the security of permutation-only ciphers [19]. It is unanimously concluded that permutation-only ciphers are broken against chosen-plaintext and know-plaintext attacks. Strong encryption with CSIS is required to convert the secret image into a meaningless encrypted image, which generates noise-like share images that do not reveal any secret information [20–22]. X. Yan et al. [23] classified the SS schemes into four security levels based on the measure of information leakage obtained from k-1 shares, where k is the threshold of the scheme. They classified CSIS as having level 3 security in which the strength of the complete algorithm depends upon the encryption method used before the application of the CSIS scheme. Z. Zhou et al. [16] proposed a modified CSIS scheme based on encrypted pixels. They employ the AES and distribute the key using the Perfect SS scheme. But their modified scheme is highly sensitive to a one-bit error during transmission and uses AES, which is not suitable for image encryption.

The AES, DES, and RSA are suboptimal algorithms for image encryption because of the inherent differences between text and image data [24]. Images are considered as voluminous multimedia and are characterized by properties like high redundancy and strong correlation between pixels [25,26]. Images can also withstand minor changes and tampering imperceptibly [27–29]. This property is not exploited by text encryption algorithms. Furthermore, large keys need to be shared among communicating parties before the actual transmission of data. In contrast, chaotic systems generate strong encryption algorithms because they offer highly aperiodic behavior [30,31]. Many chaos-based algorithms have been proposed over the last decade because of the advantages like high randomness, ergodicity, intense dependence on initial conditions, and parameters [32]. The traditional chaos-based ciphers offer double-layer security, following a confusion-diffusion architecture. This method is a composition of pixel permutation and value substitution, leading to a robust encryption technique. The 1-D chaos-based algorithms are simple to implement and can be effectively utilized for image encryption [33]. However, there are several disadvantages of using an algorithm that entirely depends on 1-D chaotic systems. These disadvantages include an exhibition of chaotic behavior within a limited range, less robustness against cryptanalytic attacks like phase-space reconstruction, nonuniform distribution of generated PRN sequence, simpler dynamical behavior, less security, and a reduced keyspace. In contrast, hyperchaotic systems have complex dynamical behavior, larger keyspace, and better key sensitivity and are difficult to decipher. Hyperchaotic systems are characterized by two positive Lyapunov exponents and are highly unpredictable [34]. Because of these strengths and desirable properties, many hyperchaos-based algorithms have been proposed recently. Furthermore, many hybrid encryption algorithms that combine DNA encoding with chaos are being proposed increasingly. DNA algorithms employ a DNA encoding method in which the secret image is converted into DNA sequences that undergo genetic manipulations and are then converted back to image format for storage. As an example, K. Zhan et al. [35] proposed an image encryption algorithm based on DNA sequences and the hyperchaotic system. In their proposed method the image is globally scrambled to achieve substitution as well as a permutation of the image pixels. This method greatly enhances the security of the proposed cryptosystem. They propose to apply the PRN sequence generated by the hyperchaotic system to all the underlying processes of the algorithm. It is evaluated that the algorithm is strong against noise attacks but has a very low Number of Pixel Change Rate (NPCR) value. Furthermore, the algorithm does not produce completely uniform histograms when applied to medical images.

Recently many research works have been proposed to study the dynamical properties of chaotic systems and have been exploited for image encryption [36,37]. For instance, Xu et al. [38] presented a scheme based on bit-level swapping permutation and diffusion. However, their scheme has a weak diffusion mechanism. Hybrid encryption algorithms utilizing chaos with DNA encoding provide enhanced security [39–41]. For example, Q. Lu et al. [42] presented an efficient image encryption method utilizing the LSS chaotic map and S-box, which increases the computational complexity. X. Deng et al. [43] combined the pixel permutation with pixel bit scrambling to improve the correlation coefficient. B. Mondal et al. [44] proposed a light-weight image encryption method based on a cross-coupled logistic map and reversible DNA encoding. Their method requires less computational overhead and can resist differential and statistical attacks. Furthermore, their algorithm uses a lower-dimensional chaotic map, as such the keyspace is lesser than the high-dimensional chaotic maps. Ye et al. [45] presented a self-adaptive image encryption method using a pre-modular operation and a chaotic intertwining logistic map. In their scheme, the keystream used for diffusion is dependent on the plain-image and therefore the algorithm can resist know-plaintext and chosen-plaintext attacks. Hu et al. [46] proposed a novel hyper-chaos image encryption method in which a pseudo-random sequence is utilized to generate the cipher image by cyclic operation and XOR-operation to transpose the pixels. C. Song et al. [47] presented a scheme that is based on DNA encoding and spatiotemporal chaos. However, the applicability of most of these encryption methods is not evaluated on medical images that have a non-homogeneous intensity distribution. Major limitations of the discussed works are summarized as follows:

- Most of the techniques have a good performance on natural images but provide non-uniform histograms for medical images.
- The output of the conventional cryptosystem is a single cipher image that can be damaged in storage and transmission.
- Many of the research works employ the lower dimensional chaotic maps, decreasing the keyspace.
- The residual image problem in CSIS is removed using AES in previous works.

We consider the highlighted disadvantages of the existing techniques by presenting our scheme that works equally well with natural and medical images. Our scheme is resistant to single-point failures, has better keyspace, and uses a computationally efficient mechanism to remove the residual image problem in CSIS.

3. COVID-19 and need for security framework

Clinical images of patients form a huge percentage of the Big Data in healthcare. In this COVID-19 crisis [48], IoMT can be used to remotely consult a specialist for virtual-care of the patients. IoMT utilizes smart sensors, processing devices, and wireless connectivity to provide real-time and efficient communication between patients and healthcare professionals. The medical image analysis, classification, and segmentation are performed to provide diagnosis, prognosis, monitoring, and possible treatment. An integrated diagnostic platform making use of Artificial Intelligence, networked infrastructure, and a security framework can help in assisting radiologists to provide quality care to many patients. The CT-Scans of COVID-19 patients show artifacts of Pneumonia even before the result of real-time reverse transcription-polymerase chain reaction (RT-PCR). Furthermore, the RT-PCR in some cases can also provide false negative tests. Therefore, the CT-scan has been identified as a predominant tool for COVID-19 diagnosis, screening, and measurement of severity of the disease. In this scenario, medical image analysis along with security of the medical data can be integrated for efficient virtual-care consultation. Encryption with CSIS can help improve the security and efficiency of the overall IoMT-based e-health system. Furthermore, conversion of the medical image into small-sized shares can be distributed and incorporate fault-tolerance. This reduces the burden on a single storage device, transmission line, and server for storage and transmission of the data and consequently helps in the Big Data management. In this work, we have utilized the chaotic and hyperchaotic systems, DNA encryption, and CSIS scheme to provide security to the medical images. These techniques have been described in detail in Section 4.

4. Preliminaris

4.1. Chaotic and hyperchaotic systems

Chaos is a deterministic pseudorandom phenomenon occurring in non-linear dynamical systems. The confusion and diffusion mechanisms employed in encryption algorithms can be implemented by chaos-based mathematical equations. The encryption algorithms based on chaos employ the PRN sequence generated by the system to perform operations like pixel position permutation and value substitution. Permutation and substitution methods reduce the inter-pixel correlation and increase the diffusion and confusion measure of the algorithm to generate robust cipher images. There are 1-D chaotic maps like logistic map, Chebyshev map, and higher dimensional maps such as Chen's hyperchaotic map. Hyperchaos arises when a high-dimensional non-linear system has two or more positive Lyapunov exponents. Hyperchaotic systems have very complex dynamical behavior and are highly secure and unpredictable. They depend upon several parameters and have more initial conditions, which greatly increase the key-space. In our proposed work, we employ both the 1-D logistic map and Chen's hyperchaotic system to enhance the security of the encryption technique. Chen's 4-D hyperchaotic system is governed by a set of four non-linear equations indicated in equation set (1). The generated sequence is then used to globally scramble the input image such that bit-level substitution and permutation is accomplished in a single step [35]. The system is in hyperchaotic state when control parameters have a value of $\alpha = 35$, $\beta = 3$, $\xi = 35$, $\tau = 5$, $\lambda_1 = 1$, $\lambda_2 = 0.2$, and $\lambda_3 = 0.3$. The initial conditions are $x_1(1,1) = 0.12$, $x_2(1,1) = 0.23$, $x_3(1,1) = 0.34$, and $x_4(1,1) = 0.45$. Furthermore, the hyperchaotic sequence is pre-iterated a fixed number of times to remove the adverse effects and the time set 'h' is taken as 0.001 [35].

$$\begin{aligned}
\dot{x_1} &= \propto (x_2 - x_1) + \lambda_1 x_4 \\
\dot{x_2} &= \xi x_1 - x_1 x_3 + \lambda_2 x_4 \\
\dot{x_3} &= -\beta x_3 - x_1 x_2 + \lambda_3 x_4 \\
\dot{x_4} &= -\tau x_1
\end{aligned} \tag{1}$$

The system is iterated M×N times with every iteration the state variables x_1^j, x_2^j, x_3^j and x_4^j are calculated, to form two key sequences $(S_i^a)^j$ and $(S_i^b)^j$. Here 'j' represents the index of operation [35]. The calculated values are concatenated to form S^j, as shown in equation (2), where i = 1,2,3,4 and $(S_i^a)^j, (S_i^b)^j \in [0, 255]$. The Pseudorandom key sequence 'k' is formed by concatenating the S^j sequences as shown in equation (3):

$$S^j = [(S_1^a)^j, (S_2^a)^j, (S_3^a)^j, (S_4^a)^j, (S_1^b)^j, (S_2^b)^j, (S_3^b)^j, (S_4^b)^j \tag{2}$$

This sequence is sorted to form k^x and used to change the position of every bit in the binary image sequence which decreases the correlation coefficient and improves security. Where 'k_i' is used to represent one element of 'k' and 'i' ∈ [1, 8×m×n].

$$k = [S^1, S^2, S^3, \ldots, S^{m\times n}] \tag{3}$$

Table 1
DNA Encoding Rules.

Rule	1	2	3	4	5	6	7	8
A	00	00	01	01	10	10	11	11
T	11	11	10	10	01	01	00	00
C	01	10	00	11	00	11	01	10
G	10	01	11	00	11	00	10	01

Table 2
DNA Addition Rules.

Addition	A	G	C	T
A	A	G	C	T
G	G	C	T	A
C	C	T	A	G
T	T	A	G	C

4.2. Logistic equation

A discrete-time non-linear system can be modeled by the 1-D logistic map represented by the mathematical equation (4). When the initial conditions x_k and μ change slightly, the resulting chaotic sequences are highly uncorrelated and spread over the entire space.

$$\begin{aligned}
&x_{k+1} = \mu x_k (1 - x_k) \\
&\quad x_k \in (0, 1) \textit{ and } \mu \in (0, 4)
\end{aligned} \tag{4}$$

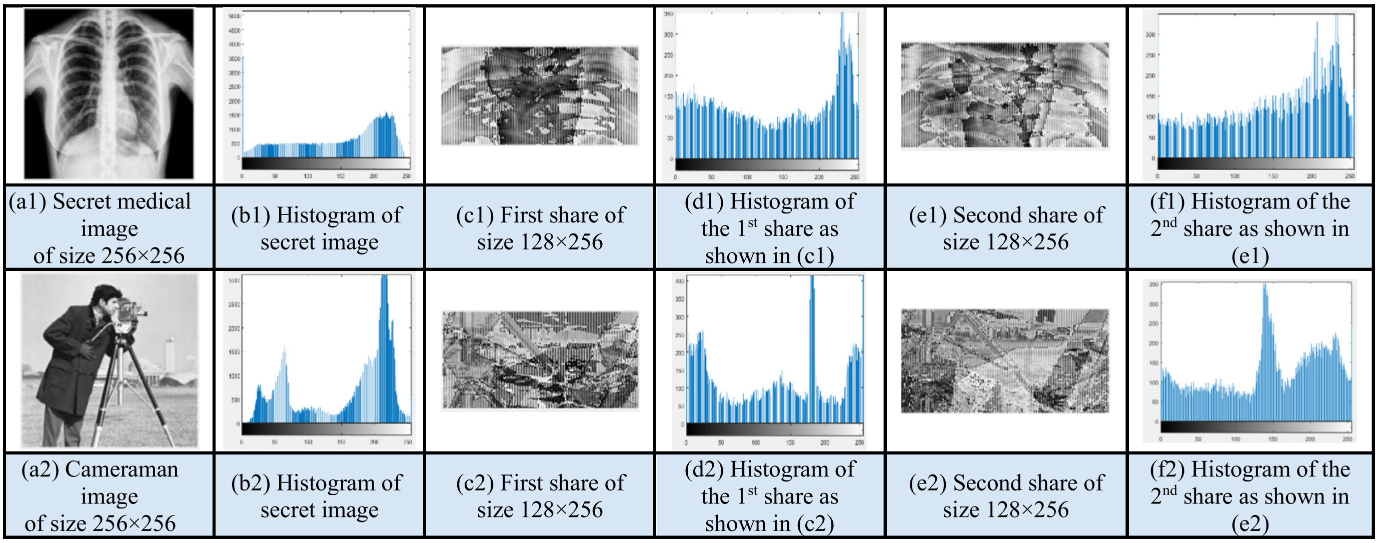
It is observed that the system is in a chaotic state when the control parameter μ is between 0 to 3.9. We take μ equal to 3.6 and iterate the equation to generate the first PRN sequence, which is XORed with the image sequence. Subsequently, the sequence is again XORed with the second uncorrelated PRN sequence generated by changing the value of μ to 3.7. The map is iterated M×N times, representing the size of the image. This greatly enhances the security level and the diffusion mechanism of the algorithm.

4.3. DNA encryption

There are many advantages of using DNA computing for image encryption, which include massive storage capability, extremely low power requirement, and parallelism [49]. DNA sequence consists of 4 bases called nucleotides namely Thymine (T), Cytosine (C), Guanine (G), and Adenine (A) [50,51]. The base A always forms a pair with T in the DNA molecule. In other words, A is complementary to T, and G is complementary to C. In digital systems 0 is complementary to 1 therefore, in a 2-bit sequence 00 will be complementary to 11, and so on [52]. Only 8 out of the 24 DNA encoding rules follow this Watson-Crick complementary rule [53]. In our proposed framework, the scrambled image is converted into DNA bases using any one of the 8 encoding rules. If the image sequence has a length equal to M×N, then the binary sequence is supposed to be 8×M×N and the DNA sequence to be 4×M×N in length. The 8 DNA encoding (DNAcode) rules are represented in Table 1. For DNA encoding rule 1 the DNA bases can be added (DNAadd) and subtracted (DNAsub) based on the binary rules illustrated in Table 2 and Table 3. The encryption algorithm utilizes an initial DNA base key d0 = 'A', which is used for DNA addition [35].

4.4. Computational secret image sharing scheme

The (k, n) threshold schemes are developed to convert secret data into n shares such that any threshold k number of shares can be pooled together to recover the complete secret. However, if fewer than k shares are combined, the participants will not be able


(a1) Secret medical image of size 256×256

(b1) Histogram of secret image

(c1) First share of size 128×256

(d1) Histogram of the 1st share as shown in (c1)

(e1) Second share of size 128×256

(f1) Histogram of the 2nd share as shown in (e1)

(a2) Cameraman image of size 256×256

(b2) Histogram of secret image

(c2) First share of size 128×256

(d2) Histogram of the 1st share as shown in (c2)

(e2) Second share of size 128×256

(f2) Histogram of the 2nd share as shown in (e2)

Fig. 2. (a1, a2) Secret images. (b1, b2) Histograms of the Secret images. (c1, c2, e1, e2) Generated shares using (2, 2) Thein and Lin's CSIS scheme. (d1, d2, f1, f2) Histograms of the share images.

Table 3
DNA Subtraction Rules.

Subtraction	A	G	C	T
A	A	T	C	G
G	G	A	T	C
C	C	G	A	T
T	T	C	G	A

to ascertain any information about the secret. The CSIS scheme developed by Thien and Lin can be used to generate share images that are 1/threshold times the size of the secret image. This scheme has the advantages of fault-tolerance and fast transmission, which is desirable in IoT-based systems. But it also suffers from several drawbacks, which need to be improved. These include a slower secret reconstruction process, more computational complexity, and residual image problem. In the CSIS scheme, the shares are generated using a sharing polynomial as shown in equation (5).

$$\boldsymbol{f}\,(\boldsymbol{x}) = \boldsymbol{a_0} + \boldsymbol{a_1 x} + \ \boldsymbol{a_2 x^2} + \cdots + \boldsymbol{a_{k-1} x^{k-1}} \quad \boldsymbol{mod\ p}. \tag{5}$$

Herein coefficients a_i, where a_i can be $a_0, \ldots .a_{k-1}$, are pixels of one block in the secret image. The scheme also uses 'p' as a large prime number (p $> a_i$) so that the resultant values are in the range 0-(p-1). The value of 'x' is substituted and a value for $f(x)$ is obtained as share pixel i.e., we get $(x_i, f(x_i))$, where $1 \le i \le n$ for the i^{th} share. The share images have a residual image problem that hampers the security condition. This is completely removed by first encrypting the secret image using a strong algorithm. The algorithm developed in this paper completely mitigates the residual image problem and the security condition is prevented from being hampered. The secret reconstruction is achieved by solving a system of linear equations. The time taken to recover the secret image is high but employing IoT-based systems along with Graphics Processing Units (GPUs) can help in solving this problem completely. Fig. 2 shows the residual image problem of the CSIS scheme observed in the shares and their corresponding histograms.

5. The proposed method

In the proposed scheme, as a first step, an input X-Ray or CT image from a COVID-19 patient is converted from decimal to binary form and all the bits are scrambled globally using the hyperchaotic system shown in equation (1) and Algorithm 1 [35]. This is explained as follows. Pixel intensity values of the grayscale image are converted into binary form to make a 1-D vector b^0. The PRN sequence k generated with the help of equation (1), (2), and (3) is sorted to form another sequence k^x. All the bits of the sequence b^0 are permuted according to the index value k^x, which is called Global Bit Scrambling (GBS) as shown in equation (7) in Algorithm 1. This greatly enhances the diffusion and substitution performance of the encryption technique. The scrambled binary sequence is represented as b^1. This sequence b^1 is converted into a string of DNA bases d^1 using one of the 8 binary coding rules as shown in Table 1. Afterward, with the help of the key DNA base 'd0', the DNA bases of d^1 are added to form d^2 using the DNA addition rules shown in Table 2. The first element (d_1^2) of this new sequence d^2 will be formed by the addition of the DNA base d0 and the first element of d^1. The rest of the elements are formed by the addition of the previous element (d_{i-1}^2) of d^2 with the current element (d_i^1) of d^1 [35]. This is shown in the equation set (6).

$$\boldsymbol{d_1^2} = \boldsymbol{d0} + +\boldsymbol{d_1^1}$$

$$\boldsymbol{d_i^2} = \boldsymbol{d_{i-1}^2} + +\boldsymbol{d_i^1}, \quad \boldsymbol{where\ i} \in [\boldsymbol{2}, \boldsymbol{4m} \times \boldsymbol{n}] \tag{6}$$

The DNA sequence is subsequently decoded into binary form b^3, which is then converted into a decimal number sequence D^1 within the range 0-255. The 1-D logistic map as in equation (4) is iterated M×N times, where M×N is the size of the image. This sequence X_1 is XORed with D^1 to form D^2. Then the parameter μ of the logistic equation is changed slightly and again iterated to generate a new sequence X_2. This is XORed with D^2 leading to the final encrypted sequence D^3. The sequence is reshaped into an M×N matrix A. This simple application of XOR operation greatly enhances security without increasing the computational complexity. Subsequently, the encrypted image is converted into share images using the CSIS scheme for distributed storage of Big Data. It is experimentally evaluated that the resultant cipher image is completely noise-like and more robust to statistical attacks. This encryption technique is equally applicable to natural as well as medical images. The experimental evaluation also validates the strength of the image shares against many attacks. The proposed method is described as Algorithm 1 and the reverse process is given in Algorithm 2.

Algorithm 1 Image encryption using hyperchaos, logistic equation, DNA encryption, and Thien and Lin's CSIS.

```
Input: Grayscale $m \times n$ secret image (I), encryption keys, (k, n) parameters, and prime number p
Step 1: Take an input image I, iterate equation (1), (2), and (3) to obtain k.
        $k^x = sort\ (k, \text{'ascending'})$
Step 2: Perform GBS of I via $\mathbf{k^x}$ as index as shown in equation (7), by first converting to binary vector $b^0$.
        $b^0 \leftarrow dec2bin(I)$
        For $j = 1$ to $m \times n \times 8$
            $b^1(j) = b^0(k^x)$        (7)
        End
Step 3: Generate DNA sequence $d^1$.
        $d^1 \leftarrow DNAcode(b^1)$, where $DNAcode(.), DNAadd(.), DNAsub(.)$, and $DNAdec(.)$ are represented in Section 5, and Tables 1, 2, and 3.
Step 4: Generate sequence $d^2$ using equation (6).
        $d_1^2 \leftarrow DNAadd(d0, d_1^1)$
        For $i = 2$ to $4 \times m \times n$
            $d_i^2 \leftarrow DNAadd(d_{i-1}^2, d_i^1)$
        End
Step 5: Generate $D^1$.
        $b^3 \leftarrow DNAdec(d^2)$
        $D^1 \leftarrow bin2dec(b^3)$, where $D^1 \in$ [0-255]
Step 6: $X_1 \leftarrow$ Iterate equation (4), where $\mu = \mu 1$.
Step 7: Generate $D^2$.
        For $i = 1$ to $m \times n$
            $D^2 \leftarrow bitxor(X_1(i), D^1(i))$
        End
Step 8: $X_2 \leftarrow$ Iterate equation (4), where $\mu = \mu 2$.
Step 9: Generate $D^3$.
        For $i = 1$ to $m \times n$
            $D^3 \leftarrow bitxor(X_2(i), D^2(i))$
        End
Step 10: $A \leftarrow Reshape(D^3)$, where $size(A) = m \times n$.
Step 11: Iterate equation (5) to get shares $S_1, S_2, \ldots, S_n$. The encrypted image A is converted into small-sized shares.
        $S_1, S_2 \ldots S_n \leftarrow CSIS(A)$
Output: Image Secret Shares $S_1, S_2 \ldots S_n$.
```

Algorithm 2 Thien and Lin's Inverse CSIS and image decryption.

```
Input: Shares $S_1, S_2 \ldots S_n$, Encryption keys, (k, n) parameters, and suitable prime number p
Step 1: $D^3 \leftarrow CSIS^{-1}\ (S_1, S_2 \ldots S_k)$ using equation (5)
Step 2: $X_2 \leftarrow$ Iterate equation (4), where $\mu = \mu 2$.
Step 3: Generate $D^2$.
        For $i = 1$ to $m \times n$
            $D^2 \leftarrow bitxor(X_2(i), D^3(i))$
        End
Step 4: $X_1 \leftarrow$ Iterate equation (4), where $\mu = \mu 1$.
Step 5: Generate $D^1$.
        For $i = 1$ to $m \times n$
            $D^1 \leftarrow bitxor(X_1(i), D^2(i))$
        End
Step 6: $b^3 \leftarrow dec2bin(D^1)$.
Step 7: $d^2 \leftarrow DNAcode(b^3)$.
Step 8: Perform DNA subtraction and DNA decoding in the reverse of equation (6) to get $b^1$.
        $b^1 \leftarrow dec2bin(DNAdec(DNAsub(b^3, do)))$
Step 9: Iterate eq. (1), eq. (2) and (3) to obtain k.
        $k^x = sort\ (k, \text{'ascending'})$
    Perform inverse GBS
    For j = 1 to $m \times n \times 8$
        $b^0(k^x(j)) = b^1(j)$
    End
Step 10: $I \leftarrow reshape(bin2dec(b^0))$, where size $(I) = m \times n$.
Output: Grayscale $M \times N$ original image I
```

6. Results and discussion

The performance of the proposed method is evaluated using metrics like key sensitivity, Correlation Coefficient (CC), histogram uniformity, information entropy, and robustness towards differential attacks, among others. Several experiments are conducted on the grayscale test images using MATLAB R2017a on Windows 10 Operating system. For hyperchaotic encryption and CSIS, test images are resized to 256×256 pixels. The encrypted image is shared using the (2, 2)-CSIS. However, the number of shares can be increased to infinity in the CSIS scheme as per the application domain. The algorithm generates a noise-like encrypted image and share images of completely uniform histograms. The source of medical images is the "OPENi" database from which a few samples are shown in Fig. 3. For illustration purposes, several natural images are also taken for the experiments.

Table 4
Comparison of correlation coefficient values with existing works.

Image 256×256	Correlation	Input Image	Proposed Scheme	HC-DNA [35]	C-DNA [54]
Cameraman	horizontal	0.9329	-0.0051	0.0076	-0.0022
	vertical	0.9566	0.0016	-0.0091	-0.0012
	diagonal	0.9117	-0.0025	-0.0012	-0.0016
Peppers	horizontal	0.9733	-8.2253e-04	0.00090	-0.0025
	vertical	0.9763	-0.0028	0.0041	-0.0025
	diagonal	0.9650	0.0038	0.00079	0.0013
Barbara	horizontal	0.8271	0.0024	0.0011	0.0016
	vertical	0.9501	0.0060	0.00063	-0.00018
	diagonal	0.8310	-0.0047	-0.0038	-0.0011
Aerial	horizontal	0.9083	0.0085	-0.00099	-0.00071
	vertical	0.8891	-1.5741e-04	0.0034	0.0037
	diagonal	0.8502	4.0214e-04	0.0022	0.0024

6.1. Encryption evaluation metrics

The encryption algorithm should be able to withstand many attacks and generate noise-like cipher images. These attacks are statistical, noise attacks, brute-force attacks, and differential attacks. The secret sharing and encryption should result in images with the following characteristics:

6.1.1. Uniform histogram

Histograms of the shares generated by the CSIS scheme with the proposed encryption are completely uniform. This shows that the images can resist the statistical attacks. The shares generated with the proposed encryption are also completely random images that do not reveal any secret information as shown in Fig. 4. The histogram uniformity is compared with the scheme presented in [35] in Fig. 5. This demonstrates the applicability of the proposed method for medical images.

6.1.2. Key-space analysis, CC, and key sensitivity

The proposed technique employs a hyperchaotic system with a large number of control parameters and initial conditions. It also employs a 1-D logistic equation in two phases with two control parameters. The DNA base 'd0 = A' also forms an input key. The key-space of the algorithm is very large and as such the brute-force attack is not feasible. Furthermore, the sensitivity to encryption keys forms an efficient parameter to evaluate the strength of a cryptosystem. For the proposed encryption scheme, the initial condition is changed from $x_1(1,1) = 0.12$ to $x_1(1,1) = 0.12 + 1e - 15$ [35]. It is shown that the decrypted image with the modified key is completely meaningless, which illustrates the key-sensitivity of the encryption technique. This is shown in Fig. 6. Furthermore, the correlation coefficient represents the degree of correlation between the adjacent pixels in the cipher image. The correlation coefficient has been evaluated and compared in Table 4 and Table 5. The PSNR and correlation between secret and recovered image is shown in Table 6.

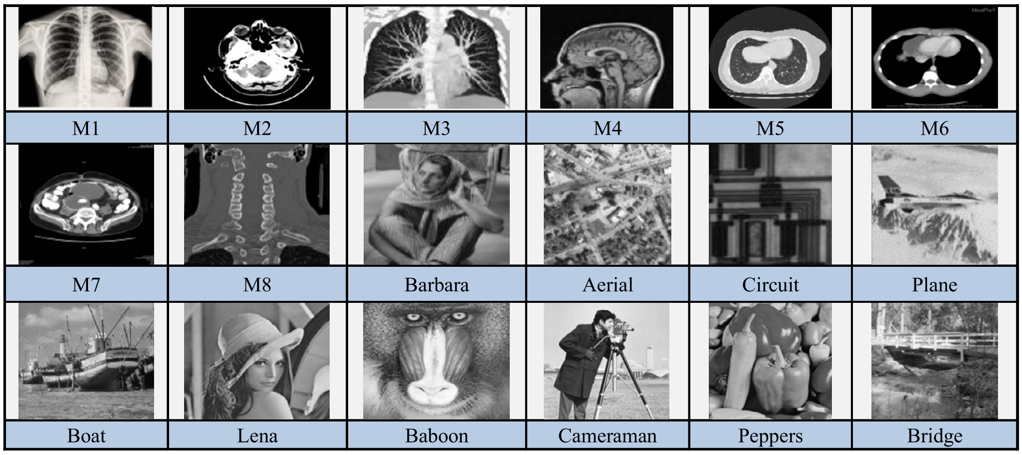


Fig. 3. Examples of test images from OPENi database (OPENi is available at https://openi.nlm.nih.gov/index.php/).

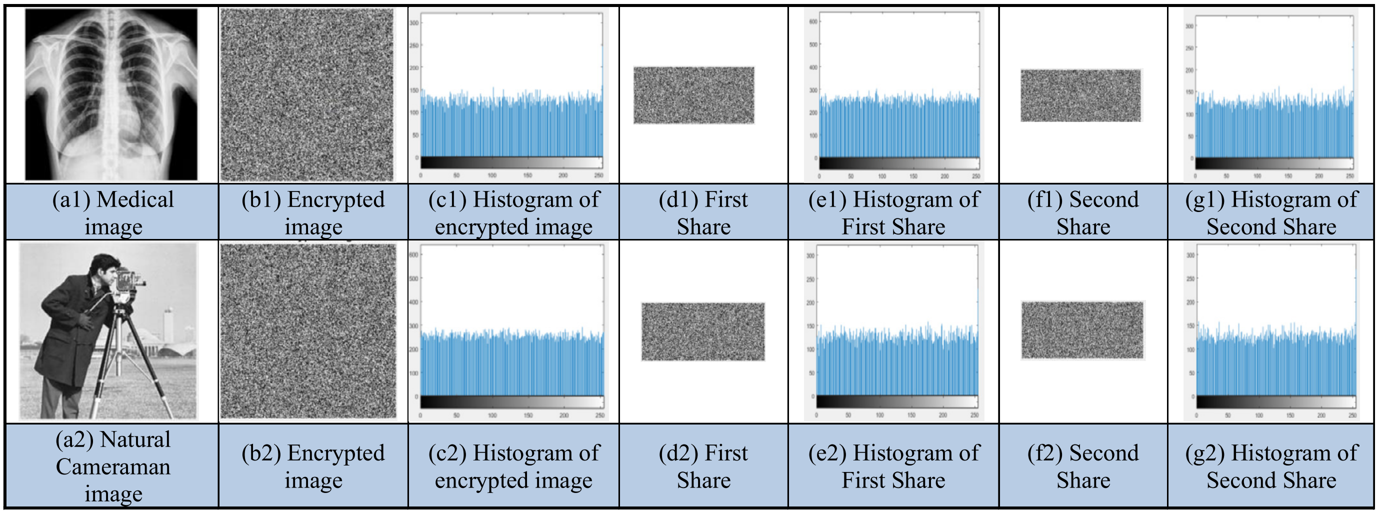

(a1) Medical image
(b1) Encrypted image
(c1) Histogram of encrypted image
(d1) First Share
(e1) Histogram of First Share
(f1) Second Share
(g1) Histogram of Second Share
(a2) Natural Cameraman image
(b2) Encrypted image
(c2) Histogram of encrypted image
(d2) First Share
(e2) Histogram of First Share
(f2) Second Share
(g2) Histogram of Second Share

Fig. 4. (a1, a2) Secret images. (b1, d1, f1, b2, d2, f2) Encrypted images and shares. (c1, e1, g1, c2, e2, g2) Histograms of encrypted images and share images.

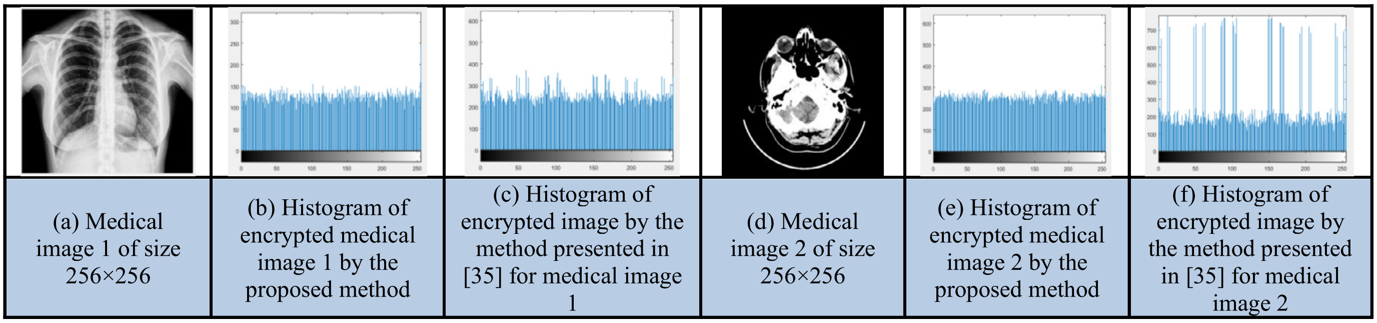
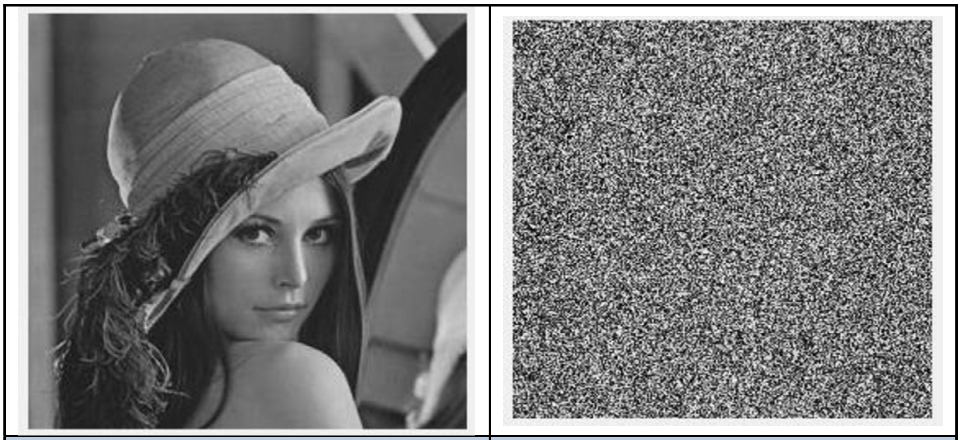

(a) Medical image 1 of size 256×256
(b) Histogram of encrypted medical image 1 by the proposed method
(c) Histogram of encrypted image by the method presented in [35] for medical image 1
(d) Medical image 2 of size 256×256
(e) Histogram of encrypted medical image 2 by the proposed method
(f) Histogram of encrypted image by the method presented in [35] for medical image 2

Fig. 5. Comparison with scheme [35] in terms of histogram uniformity for applicability to natural and medical images. (a, d) Medical images, (b, e). Histogram of encrypted images by the proposed scheme. (c, f) Histogram of encrypted images using scheme [35].

Table 5
Comparison of correlation coefficient values for Lena image with recent schemes.

Image 256×256	Correlation	Input Image	Proposed Scheme	HC-DNA [35]	C-DNA [54]	[55]
Lena	horizontal	0.9494	-0.0014	0.0019	-0.0047	0.0070
	vertical	0.9667	-0.0062	-0.0030	0.0040	-0.0102
	diagonal	0.9366	-3.9896e-04	0.0018	-0.0034	0.0030



(a) Decrypted image with Key having one initial value $x_1(1,1) = 0.12$.

(b) Decrypted image with one Key initial value changed slightly $x_1(1,1) = 0.12 + 1e - 15$

Fig. 6. Key-space analysis and sensitivity with change in initial condition $x_1(1, 1)$ from 0.12 to 0.12 + $1e - 15$ of the hyperchaotic system.

Table 6
PSNR and correlation between secret and recovered image.

Secret and Recovered Images for Proposed method	Correlation	PSNR (dB)
Lena	1	∞
M1	1	∞
Baboon	1	∞

Table 7
NPCR values for share images.

Test Images	NPCR (%) between first share images when the input image is changed by one bit.	NPCR (%) between second share images when the input image is changed by one bit.
M1	99.10	99.60
M2	98.68	99.71
M3	99.14	99.64
Lena	99.12	99.62
Baboon	99.17	99.69
Bridge	99.07	99.70
Cameraman	99.19	99.63
Peppers	99.12	99.60
Plane	99.07	99.61
Boat	99.14	99.68
M4	99.08	99.69
M5	99.05	99.65
M6	98.75	99.64
M7	98.79	99.70
M8	99.13	99.72

6.1.3. *Better diffusion characteristics*

To evaluate the diffusion characteristics, we use the parameter called NPCR as shown in equation (8) and Table 7. We calculate NPCR between the first share images and second share images, respectively, when the input image is changed by 1-bit. The NPCR value is close to the maximum theoretical limit of 99.6094% [35]. The comparison of NPCR is shown in Table 8.

$$\boldsymbol{D(i,j) = \{0,\ if\ S1(i,j) = S2(i,j)1,\ if\ S1(i,j) \neq S2(i,j)}$$

$$\boldsymbol{NPCR(S1,S2) = \sum i, j\frac{D(i,j)}{M \times N} \times 100\%} \quad (8)$$

6.1.4. *Entropy*

Entropy is a measure of the amount of randomness in the encrypted image and generated shares. The value of entropy should be close to 8 for better randomness. The information entropy is more than 7.99 for both the shares revealing the strength towards entropy attacks. The entropy values for both shares generated by the proposed scheme are comparable to the state-of-the-art schemes [35,54–57,61] and are shown in Table 9 and Table 10.

6.1.5. *SSIM*

SSIM is called an image structural similarity and its value is between -1 and +1. Ideally, the similarity score between the secret image and image shares should be zero, indicating zero similarity. The obtained results are very close to zero and are shown in Table 9, which is again comparable to most of the recent schemes [35,54–57].

7. Conclusion

The IoT empowered Big Data solutions can facilitate medical data analysis during the COVID-19 pandemic. The medical images constitute a large portion of the healthcare data and contain sensitive information about patients. For the implementation of efficient management solutions, the IoT and AI-based smart healthcare systems need to be completely secured. The CSIS scheme can be used to store the medical images on third-party cloud servers. The use of strong encryption with CSIS helps maintaining the security condition of the threshold scheme. In this paper, we proposed an encryption algorithm based on the logistic equation, hyperchaotic equation, and DNA encoding. Subsequently, we used a lossless CSIS method to convert the encrypted secret image into shares for distributed storage in IoT-based servers. We applied our algorithm to medical images as well as natural images and confirmed its withstanding capability to statistical and differential attacks compared to existing methods.

In the future, we aim to implement IoT systems along with the use of GPUs to mitigate other disadvantages of the CSIS scheme such as high computational complexity and time requirement for secret reconstruction.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Table 8
Comparison of NPCR values with state-of-the-art schemes.

Test images encrypted using the proposed algorithm	NPCR (%) between first share images.	NPCR (%) between second share images.	[55]	[57]	[58]	[60]
Lena	99.12	99.62	99.62	99.59	99.61	99.60
Baboon	99.17	99.69	-	99.61	-	-
Cameraman	99.19	99.63	-	99.60	99.60	-

Table 9
Entropy and SSIM values for shares.

Test Images	The entropy of 1st share	The entropy of 2nd share	SSIM of secret image and 1st share	SSIM of secret image and 2nd share
M1	7.9923	7.9918	0.0079	0.0065
M2	7.9910	7.9924	0.0032	0.0036
M3	7.9921	7.9924	0.0124	0.0048
Lena	7.9917	7.9929	0.0097	0.0085
Cameraman	7.9928	7.9918	0.0104	0.0065
Barbara	7.9915	7.9926	0.0105	0.0097
Peppers	7.9921	7.9919	0.0081	0.0078

Table 10
Comparison of entropy values with state-of-the-art schemes.

Test Images	The entropy of 1st share	[59]	[56]	[57]	[61]
Lena	7.9917	7.9974	7.9894	7.9974	7.9983
Cameraman	7.9928	-	-	7.9970	-
Baboon	7.9939	-	-	7.9968	-

Acknowledgement

The authors would like to thank the Department of Science and Technology (DST) New Delhi, Government of India for providing financial support under the DST Inspire Fellowship Scheme (NO. IVR201800005281).

References

[1] F. Piccialli, G. Casolla, S. Cuomo, F. Giampaolo, V.S. di Cola, Decision making in IoT environment through unsupervised learning, IEEE Intell. Syst. 35 (1) (2020) 27–35.
[2] B. Lin, S. Wu, COVID-19 opportunities and challenges for digital health and the Internet of medical things in China, Omics. J. Integr. Biol. 24 (5) (2020) 231–232.
[3] N.N. Hurrah, S.A. Parah, N.A. Loan, J.A. Sheikh, M. Elhoseny, K. Muhammad, Dual watermarking framework for privacy protection and content authentication of multimedia, Future Gener. Comput. Syst. 94 (2019) 654–673.
[4] G. Casolla, S. Cuomo, V.S. Di Cola, F. Piccialli, Exploring unsupervised learning techniques for the Internet of things, IEEE Trans. Ind. Inform. 16 (4) (2020) 2621–2628.
[5] K. Muhammad, J. Ahmad, S. Rho, et al., Image steganography for authenticity of visual contents in social networks, Multimed. Tools Appl. 76 (2017) 18985–19004.
[6] J. Wang, K. Han, A. Alexandridis, Z. Chen, Z. Zilic, Y. Pang, G. Jeon, F. Piccialli, A blockchain-based eHealthcare system interoperating with WBANs, Future Gener. Comput. Syst. 110 (2020) 675–685.
[7] F. Piccialli, S. Cuomo, V.S. di Cola, G. Casolla, A machine learning approach for IoT cultural data, J. Ambient Intell. Humaniz. Comput. (2019) 1–12, https://doi.org/10.1007/s12652-019-01452-6.
[8] R. Hamza, Z. Yan, K. Muhammad, P. Bellavista, F. Titouna, A privacy-preserving cryptosystem for IoT E-healthcare, Inf. Sci. 527 (2020) 493–510.
[9] S. Wang, Distributed Storage based on Secret Sharing Schemes (D4S), MATLAB Central File Exchange, Retrieved March 29, 2020.
[10] K. Muhammad, J. Ahmad, N.U. Rehman, Z. Jan, R.J. Qereshi, A secure cyclic steganographic technique for color images using randomization, Tech. J. Univ. Eng. Technol. Taxila Pakistan 19 (2014) 57–64.
[11] C.C. Thien, J.C. Lin, Secret image sharing, Comput. Graph. 26 (5) (Oct. 2002) 765–770.
[12] K. Muhammad, J. Ahmad, H. Farman, M. Zubair, A novel image steganographic approach for hiding text in color images using HSI color model, Middle-East J. Sci. Res. 22 (2014) 647–654.
[13] A.M. Badshah, N. Rahim, N. Ullah, J. Ahmad, K. Muhammad, M.Y. Lee, S.L. Kwon, S.W. Baik, Deep features-based speech emotion recognition for smart effective services, Multimed. Tools Appl. 78 (2019) 5571–5589.
[14] K. Muhammad, J. Ahmad, M. Sajjad, et al., Visual saliency models for summarization of diagnostic hysteroscopy videos in healthcare systems, SpringerPlus 5 (2016) 1495.
[15] C.C. Thien, J.C. Lin, An image-sharing method with user-friendly shadow images, IEEE Trans. Circuits Syst. Video Technol. 13 (12) (2003) 1161–1169.
[16] Z. Zhou, C. Yang, Y. Cao, X. Sun, Secret image sharing based on encrypted pixels, IEEE Access 6 (2018) 15021–15025.
[17] L. Bai, A. Ortiz, D. Dalessandro, An image secret sharing method, in: 9th International Conference on Information Fusion, Florence, Italy, 2006, pp. 1–6.
[18] L. Pang, D. Miao, H. Li, Q. Wang, Improved secret image sharing scheme in embedding capacity without underflow and overflow, Sci. World J. (2015), https://doi.org/10.1155/2015/861546.
[19] A. Jolfaei, X.W. Wu, V. Muthukkumarasamy, On the security of permutation-only image encryption schemes, IEEE Trans. Inf. Forensics Secur. 11 (2) (2016) 235–246.
[20] D. Coppersmith, The data encryption standard (DES) and its strength against attacks, IBM J. Res. Dev. 38 (3) (1994) 243–250.
[21] H. Gao, Y. Zhang, S. Liang, D. Li, A new chaotic algorithm for image encryption, Chaos Solitons Fractals 29 (2) (2006) 393–399.
[22] S. Li, G. Chen, X. Zheng, Chaos-based encryption for digital images and videos, in: B. Furht, D. Kirovski (Eds.), Multimedia Security Handbook, CRC Press, Boca Raton, FL, USA, 2004, pp. 133–167.
[23] X. Yan, L. Liu, Y. Lu, Q. Gong, Security analysis and classification of image secret sharing, J. Inform. Secur. Appl. 47 (2019) 208–216.
[24] Announcing the Data Encryption Standard (DES), NIST Standard 46–3, 1999.
[25] A.A. Reshi, S.A. Parah, Performance evaluation and future scope of image secret sharing schemes, in: 2018 Fifth International Conference on Parallel, Distributed and Grid Computing (PDGC), Solan Himachal Pradesh, India, 2018, pp. 640–645.
[26] N.A. Loan, N.N. Hurrah, S.A. Parah, J.W. Lee, J.A. Sheikh, G.M. Bhat, Secure and robust digital image watermarking using coefficient differencing and chaotic encryption, IEEE Access 6 (2018) 19876–19897.
[27] M. Kurt Pehlivanoğlu, N. Duru, Encryption of Walsh Hadamard transform applied images with the AES encryption algorithm, in: 2016 24th Signal Processing and Communication Application Conference (SIU), Zonguldak, 2016, pp. 301–304.
[28] A. Chatterjee, J. Dhanotia, V. Bhatia, S. Prakash, Virtual optical encryption using phase-shifted digital holography and RSA algorithm, in: 2018 3rd International Conference on Microwave and Photonics (ICMAP), Dhanbad, 2018, pp. 1–2.
[29] A. Ray, A. Potnis, P. Dwivedy, S. Soofi, U. Bhade, Comparative study of AES, RSA, genetic, affine transform with XOR operation, and watermarking for image encryption, in: 2017 International Conference on Recent Innovations in Signal Processing and Embedded Systems (RISE), Bhopal, 2017, pp. 274–278.

[30] Z. Galias, W. Tucker, Numerical study of coexisting attractors for the H´enon map, Int. J. Bifurc. Chaos Appl. Sci. Eng. 23 (7) (2013) 1–18.
[31] K. Muhammad, R. Hamza, J. Ahmad, J. Lloret, H. Wang, S.W. Baik, Secure surveillance framework for IoT systems using probabilistic image encryption, IEEE Trans. Ind. Inform. 14 (2018) 3679–3689.
[32] Y. Li, C. Wang, H. Chen, A hyper-chaos-based image encryption algorithm using pixel-level permutation and bit-level permutation, Opt. Lasers Eng. 90 (2017) 238–246.
[33] N. Pareek, V. Patidar, K. Sud, Image encryption using a chaotic logistic map, Image Vis. Comput. 24 (2006) 926–934.
[34] L. Chunlai, Y. Simin, A new hyperchaotic system & it's adaptive tracking control, Acta Phys. Sin. 61 (4) (2012) 22–28.
[35] K. Zhan, D. Wei, J. Shi, J. Yu, Cross-utilizing hyperchaotic and DNA sequences for image encryption, J. Electron. Imaging 26 (1) (2017) 013021.
[36] N. Tsafack, J. Kengne, Complex dynamics of the Chua's circuit system with adjustable symmetry and nonlinearity: multistability and simple circuit realization, World J. Appl. Phys. 4 (2) (2019) 24.
[37] Z. Hua, Y. Zhou, Exponential chaotic model for generating robust chaos, IEEE Trans. Syst. Man Cybern. Syst. (2019), https://doi.org/10.1109/TSMC.2019.2932616, early access.
[38] L. Xu, Z. Li, J. Li, W. Hua, A novel bit-level image encryption algorithm based on chaotic maps, Opt. Lasers Eng. 78 (21) (2016) 17–25.
[39] A. Belazi, M. Talha, S. Kharbech, W. Xiang, Novel medical image encryption scheme based on chaos and DNA encoding, IEEE Access 7 (2019) 36667–36681.
[40] K.C. Jithin, S. Sankar, Colour image encryption algorithm combining Arnold map, DNA sequence operation, and a Mandelbrot set, J. Inf. Secur. Appl. 50 (2020).
[41] L. Xu, Z. Li, J. Li, A novel bit-level image encryption algorithm based on chaotic maps, Opt. Lasers Eng. 78 (2016) 17–25.
[42] Q. Lu, C. Zhu, X. Deng, An efficient image encryption scheme based on the LSS chaotic map and single S-box, IEEE Access 8 (2020) 25664–25678.
[43] X. Deng, et al., Image encryption algorithms based on chaos through dual scrambling of pixel position and bit, J. Commun. 3 (2014).
[44] B. Mondal, T. Mandal, A lightweight secure image encryption scheme based on chaos and DNA computing, J. King Saud Univ, Comput. Inf. Sci. 29 (2017) 499–504.
[45] G. Ye, X. Huang, An efficient symmetric image encryption algorithm based on an intertwining logistic-map, Neurocomputing 251 (2017) 45–53.
[46] T. Hu, Y. Liu, L.H. Gong, C.Y. Ouyang, An image encryption scheme combining chaos with cycle operation for DNA sequences, Nonlinear Dyn. 87 (2017) 51–66.
[47] C. Song, Y. Qiao, A novel image encryption algorithm based on DNA encoding and spatiotemporal chaos, Entropy 17 (10) (2015) 6954–6968.
[48] https://www.worldometers.info/coronavirus/.
[49] P. Zhen, G. Zhao, L. Min, X. Jin, Chaos-based image encryption scheme combining DNA coding and entropy, Multimed. Tools Appl. 75 (11) (2016) 6303–6319.
[50] M.R. Biswas, K.M.R. Alam, A. Akber, Y. Morimoto, A DNA cryptographic technique based on dynamic DNA encoding and asymmetric cryptosystem, in: 2017 4th International Conference on Networking, Systems and Security (NSysS), Dhaka, 2017, pp. 1–8.
[51] X. Fu, B. Liu, Y. Xie, W. Li, Y. Liu, Image encryption-then-transmission using DNA encryption algorithm and the double chaos, IEEE Photonics J. 10 (3) (2018) 1–15.
[52] Z. Zhou, D. Huang, Z. Wang, Efficient privacy-preserving ciphertext-policy attribute based-encryption and broadcast encryption, IEEE Trans. Comput. 64 (1) (2015) 126–138.
[53] J.D. Watson, F.H.C. Crick, A structure for deoxyribose nucleic acid, Nature 171 (4356) (1953) 737–738.
[54] X. Wang, C. Liu, A novel and effective image encryption algorithm based on chaos and DNA encoding, Multimed. Tools Appl. 76 (5) (2017) 1–17.
[55] X. Chai, et al., Medical image encryption algorithm based on Latin square and memristive chaotic system, Multimed. Tools Appl. 78 (2019) 35419–35453.
[56] T. Li, B. Du, X. Liang, Image encryption algorithm based on logistic and two-dimensional Lorenz, IEEE Access 8 (2020) 13792–13805.
[57] Y. Wan, S. Gu, B. Du, A new image encryption algorithm based on composite chaos and hyperchaos combined with DNA coding, Entropy 22 (2) (2020) 171.
[58] L. Xu, X. Gou, Z. Li, J. Li, A novel chaotic image encryption algorithm using block scrambling and dynamic index-based diffusion, Opt. Lasers Eng. 91 (2017) 41–52.
[59] L. Xu, Z. Li, J. Li, W. Hua, A novel bit-level encryption based on chaotic maps, Opt. Lasers Eng. 78 (2016) 17–25.
[60] S.S. Askar, A.A. Karawia, A. Al-Khedhairi, F.S. Al-Ammar, An algorithm of image encryption using logistic and two-dimensional chaotic economic maps, Entropy 21 (44) (2019).
[61] F.P. An, J.E. Liu, Image encryption algorithm based on adaptive wavelet chaos, J. Sensors 2019 (Dec. 2019) 1–12.