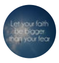
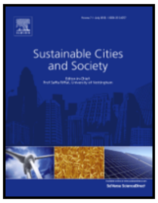
Secret Sharing-based Personal Health Records Management for the Internet of Health Things



Contents lists available at ScienceDirect

Sustainable Cities and Society

journal homepage: www.elsevier.com/locate/scs



Secret Sharing-based Personal Health Records Management for the Internet of Health Things

Parsa Sarosh [1], Shabir A. Parah [1], G. Mohiuddin Bhat [2], Ali Asghar Heidari [3], [4], [1], Khan Muhammad [5], *

[1] Post Graduate Department of Electronics and Instrumentation Technology, University of Kashmir, Srinagar, India
[2] Department of Electronics and Communication Engineering, Institute of Technology, Zakoora, India
[3] School of Surveying and Geospatial Engineering, College of Engineering, University of Tehran, Tehran, Iran
[4] Department of Computer Science, School of Computing, National University of Singapore, Singapore
[5] Department of Software, Sejong University, Seoul 143-747, Republic of Korea

ARTICLE INFO

Keywords:
Big Data
IoHT
Cloud Computing
Sustainability
Smart city
Medical Data Security
e-Healthcare
RC6 Encryption
Secret Image Sharing
Personal Health Record

ABSTRACT

The holistic concept of smart cities has been adopted to increase economic, environmental, and social sustainability. For the sustainable health of a smart city inhabitant, there is a requirement for innovations in implementing health solutions. Given the exponential growth of the Internet of Health Things (IoHT) in health infrastructures, bulk amounts of health-related data are accumulated in Personal Health Records (PHR) and processed in storage data centers. One of the major challenges in this scenario is the security of this enormous medical data. The conventional encryption schemes generate single cipher images making the cryptosystem vulnerable to single-point attacks. This paper evaluates a distributed security module for the clinical images that form 80% of the health data. We utilize the Rivest Cipher 6 (RC6) encryption algorithm with the Computational Secret Sharing Scheme (CSIS) scheme for distributed storage of clinical images. The key is shared using the Perfect Secret Sharing scheme (PSS). We show that (k-1) key-shares and the 'n' image shares can be made public because of the perfect security of the scheme. The rest of the key shares can be secured using the Deoxyribonucleic Acid substitution (DNA substitution) method. Analysis of the shares generated reveals the strength of the cryptosystem and gives an insight into the degree of security provided to the health-related data. The entropy of the generated shares is higher than 7.99, and structural similarity (SSIM) values are negligible. The Number of Pixels Change Rate (NPCR) values are greater than 99.55% for all the shares that show a high diffusion measure. Comparison with state-of-the-art schemes reveal and validate the robustness of the cryptosystem

1. INTRODUCTION

A smart city is regarded as an innovative and intelligent system of interconnected infrastructures, including Information and Communication Technology (ICT), economic, and social frameworks [1]. This holistic approach to the concept of cities aims at improving the standard of living of a smart city inhabitant. This is achieved by remodeling major sectors like economy, telecommunication, transportation, and healthcare. Sustainable healthcare infrastructure is imperative for the citizens of smart cities. A smart city aims to provide solutions for sustainable health with the help of technological innovations like Artificial intelligence, IoHT, and communicating devices [2]. IoHT is a network of sensors and devices that are connected via the internet for the collection, processing, and analysis of health data. This data can subsequently be used for patient monitoring, remote consultation, diagnosis, and treatment.

G. Palozzi et al. (2020) [3] present a detailed analysis of the advantages of IoHT-based smart healthcare. They elaborate on the theoretical and empirical aspects highlighting the real potential and security lacunas in the IoHT implementation. A. Mukherjee et al. (2021) [4] present an IoHT healthcare module utilizing the cloud, fog, and edge computing frameworks. Furthermore, they present a model to predict the patient's mobility and demonstrate improvement over the cloud-only healthcare models. PHRs are an innovative outcome of the increasing growth of IoHT in smart, sustainable cities. These records contain various forms of data like structured and unstructured, coming from multi-

* Corresponding Author.
E-mail addresses: as_heidari@ut.ac.ir, aliasgha@comp.nus.edu.sg, t0917038@u.nus.edu (A.A. Heidari), khan.muhammad.icp@gmail.com (K. Muhammad).

[1] https://aliasgharheidari.com

https://doi.org/10.1016/j.scs.2021.103129
Received 22 February 2021; Received in revised form 30 May 2021; Accepted 30 June 2021
2210-6707/© 2021

ple sources like wearable devices, mobile phones, etc. Big Data analysis is often required to gain valuable insights into these large volumes of health data [5]. A security framework is required for sustainable health to make IoHT and data-driven solutions more secure [6]. This will bring revolutionary changes in the clinical environment and help gain the trust of an urban city inhabitant [7]. For diagnostic purposes, an IoHT aims to provide easy and timely access to high-resolution medical images [8]. However, the challenge lies in making the content available in the most secure manner to all the concerned stakeholders [9, 10].

In this data-intensive IoHT ecosystem, providing security and privacy can be a very complex and challenging task. A tremendous number of data breaches of PHRs have been reported in the last few years. According to the data provided by Health IT security, 41.4 million PHRs were breached in the year 2019. Aveanna healthcare and PIH Health reported that the data of 166077 and 200000 patients were hacked using phishing attacks in 2019. Quest Diagnostics reported that the PHRs of nearly 12 million patients were hacked, and Canada's Lifelabs disclosed that 15 million PHRs were breached from their databases in 2019. In September 2020, Trinity Health suffered a data breach exposing the records of 3320726 patients. Apart from the ones mentioned above, many more cases of PHRs data breach have been reported in the last few years. The above statistical details serve as a motivating factor for many researchers to devise improved algorithms for data security. Improved data management can be achieved with increased security and safeguards against potential security threats like data breaches or malicious attacks. Several security modules have been developed over the past decade for the clinical images that form 80% of the health data.

To secure sensitive medical information, steganography [11], digital watermarking [12], and encryption methods are often utilized [13]. Secret sharing (SS) schemes have also emerged as an efficient tool for data protection [14]. Steganography can be employed in the SS process to authenticate the shares given to the participants. Many research works have been proposed to combine SS with steganography to strengthen the cryptosystem [15]. The PHR data should be distributed to different IoHT cloud servers to avoid storage at a single point [16]. IoHT-based PHR systems provide numerous benefits to the patient, doctors, and healthcare centers like the ease of authorized access [17, 18], smart monitoring [19], key management, well-organized storage, enhanced security [20], and less dependence on the local storage devices [21]. PHRs are generally outsourced to be stored at a third party, such as the IoHT service provider [22]. This exposes the unencrypted PHR to the cloud administrators and can lead to unauthorized access. Regarding sustainable health, the PHR needs to be encrypted before transferring the data to distributed storage points. Therefore, medical data security is essential for sustainable health solutions for the citizen of a smart city and a smart society.

CSIS has been found to store the PHRs at distributed IoHT servers efficiently because of properties like fault tolerance and reduced share size. Using the CSIS scheme, the PHR data can be distributed, and single-point attacks can be removed entirely. If one of the shares is corrupted by noise during transmission or storage, then the complete secret can be reconstructed using other shares. Furthermore, the number of shares can be generated to infinity using the CSIS scheme and can be used to update the SS scheme. For example, if the patient and doctor are in the SS process and the owner of the healthcare center needs to gain access to the PHR, then using the CSIS scheme, he can be provided with a share.

The CSIS can recover the data in a lossless manner, particularly in the healthcare scenario where medical images carry most of the information. However, the disadvantage of using this scheme is that the complexity is more and the generated shares exhibit certain patterns and reveal slight details about the secret image [23]. This problem arises because of the inter-pixel redundancy normally seen in medical images and hampers the security condition of the threshold scheme. This is known as a residual image problem and can be mitigated using known encryption techniques. With the help of encryption, the generated shares will become noise-like, and no information will be revealed. The data encryption [24], SS, and DNA substitution methods [25] can be utilized in concurrence to distribute the PHR data securely onto multiple cloud servers. Encryption methods like RC6 encryption [26, 27], logistic equation [28], Data Encryption Standard [29], and chaos encryption [30, 31] can be employed in combination with CSIS to provide enhanced security. Improved encryption techniques can be developed to mitigate the residual image problem efficiently.

The cloud service provider receives encrypted-PHR and would distribute it on the semi-trusted IoHT-based cloud servers using the CSIS scheme, as shown in Fig. 1. When the PHR needs to be retrieved, the cloud service provider reconstructs the encrypted PHR and sends it to

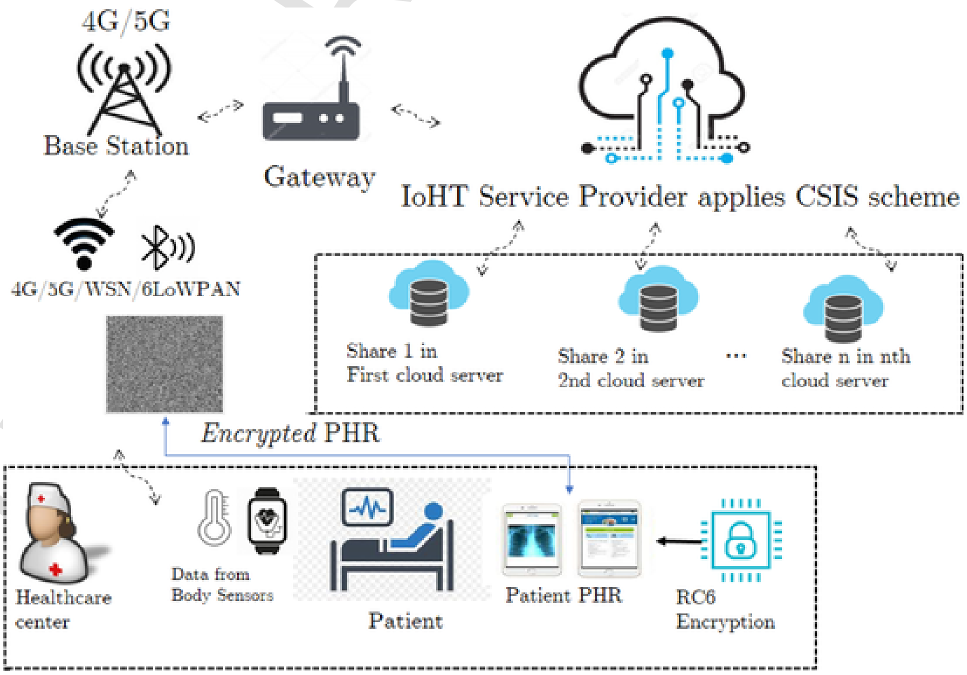


Fig. 1. PHR data storage in Cloud Servers on IoHT.

the healthcare center. Subsequently, PHR is decrypted by the authorized healthcare center using the key. The main contributions of our paper are enlisted as follows:

- The presented technique produces completely noise-like image shares and key shares distributed onto multiple servers in an IoHT-based framework. This prevents single-point attacks on the cryptosystem.
- The scheme generates small-sized shares, which reduce the bandwidth and memory requirement for single share transmission and storage, respectively. Furthermore, the application of the PSS scheme for secret-key distribution is illustrated in detail.
- The scheme offers perfect security wherein 'n' image shares and (k-1) key shares can be transmitted via an unsecured channel.
- The presented scheme recovers the medical data in a lossless manner, which will help in data analysis and diagnosis in IoHT.

The layout of our paper is arranged as follows. Section 2 summarizes the review of relevant DNA encryption and SS schemes as per the available literature. Section 3 illustrates the CSIS scheme and its issues. Section 4 presents the proposed security model. Results and Discussion are presented in Section 5. Section 6 presents the conclusion of the research work.

2. LITERATURE REVIEW

Due to massive urbanization presently, more than 4 billion people are living in urban areas. U.N estimates that around 55% of the world population live in cities and has further estimated the percentage to increase to 68% by 2050. B. N. Silva et al. (2018) [32] present an overview of smart sustainable cities. They describe the characteristics, composition, and implementation of smart cities. According to them, the characteristics of smart cities include sustainability, smartness, Quality of Life, and Urbanization. They further illustrate that smart health, smart community, smart transportation, and smart energy form the major components of a smart city. Due to the exponential population increase, cities cannot handle the increased healthcare demand of the urban citizens. To cater to the large population smart and sustainable healthcare solutions are to be deployed. The optimized healthcare services use ICT, IoHT, sensors, Edge computing, and Artificial Intelligence, among others [33]. To provide sustainable healthcare facilities, data security has become the most relevant area of research. Several researchers have proposed to store e-health data onto IoHT-based servers with pivotal importance to security, privacy, and fine-grained access. G. G. Dagher et al. (2018) [34] present a security framework based on blockchain technology. In their proposed scheme, cryptographic techniques are used to provide security, and Ethereum-based blockchain is used to provide access control and obfuscation of medical data. The scheme can be used for interoperable and secure access to PHRs by patients and healthcare providers. They developed a framework called Ancile, and its performance to security and privacy concerns of smart healthcare systems are thoroughly evaluated.

Several DNA cryptography-based schemes have been presented for data encryption. X. Wang et al. (2017) [35] present an encryption scheme that utilizes the Piecewise Linear Model (PWLM), logistic map, and DNA encryption. Their scheme generates a key image using the PWLM and encodes the image row by row using different DNA encoding rules. The logistic equation decides the particular DNA rule, and the process is repeated for the columns of the image. It is seen that the encryption algorithm is not highly sensitive to the encryption key. X. Wang et al. (2018) [36] propose a new image encryption technique that employs DNA confusion using the Lorenz system. The technique utilizes the DNA operations and permutation to distort the bit planes of the plain image. X. Wu et al. (2018) [37] present an image encryption scheme using one-time keys, spatiotemporal maps, and DNA sequences. The key-streams are generated using the NCA map-based CML, and the hash function SHA-256 is calculated. Several DNA operations like DNA addition, DNA subtraction, and DNA XOR operations are performed to get the final encrypted image. J. Wu et al. (2018) [38] propose a new 2D Henon-Sine map (2D-HSM) and an encryption scheme based on this map. They apply DNA operations for pixel diffusion, and the 2D-HSM is utilized for pixel permutation. The 2D map has been evaluated using phase diagram, bifurcation diagram, and Lyapunov exponent. However, the keyspace of the algorithm is lower than the hyper-chaotic systems.

Rehman et al. (2019) [39] present a color image encryption scheme that is based on confusion and dual diffusion. To safeguard against differential and statistical attacks, they employ chaotic systems, DNA encoding, and a 2D logistic map. In their scheme SHA-256 hash is calculated to change the initial conditions of the 2D map. S. Zhu et al. (2020) [40] develop a continuous 5D hyperchaotic system and an encryption scheme based on it. In their proposed scheme the rules of DNA coding change dynamically according to the pixel value. They also perform pixel-level permutation in two rounds which increases the confusion measure of the algorithm. The scheme generates a keystream using the 5D hyper-chaotic system and DNA conversion, increasing the time and computational complexity. Several other DNA-based encryption schemes have been presented which impart security to the images and the encryption keys [41]. Several SS schemes, including the boolean-based SS, and counting-based SS have been recently proposed [42]. The counting-based SS makes use of 1-bit and 2-bits combination techniques to generate the secret shares. Furthermore, SS can also be combined with steganography to hide the existence of a secret or authenticate the generated shares [43]. Among the many variants of SS schemes, the lossless CSIS scheme provides several advantages like generation of small-sized shares, fault tolerance, fast transmission, lossless recovery, and secure communication, among others.

The CSIS technique developed by Thein and Lin (2003) [44] makes use of pixel permutation to deal with the residual image problem and uses the number 251 as the prime number in the sharing process. This leads to lossy-recovery of the secret image as all the values above 250 are truncated. K. S. Wu (2013) [45] propose a method for lossless image recovery by replacing the prime number by 257 to preserve the light pixels. A. Jolfaei et al. (2016) [46] reveal that permutation-only ciphers are broken against chosen-plaintext attacks. The number of plain and cipher image pairs required to break the permutation-only cipher are$n = log_L [MN]$, where 'L' represents the intensity values and 'M × N' is the size of the image. Permutation causes a change in the position of the pixels and does not change the histogram of the image, making the algorithm weak against statistical attack. Therefore, as the CSIS scheme proposed by Thein and Lin permutes the secret image before initiating the SS process, this scheme is highly vulnerable to attacks. D. Xie et al. (2017) [47] propose a method to improve the noise tolerance, flexibility, and scalable recovery of the secret image by compressed sensing.

W. Ding et al. (2018) [48] present a method to recover the secret image in a completely lossless manner for the PSS scheme. X. Zhou et al. (2018) [49] present a modified Thein-and-Lin's sharing scheme by taking two adjacent pixels as a secret term and a prime number equal to 65537. However, as with most of the other schemes, they also employ permutation before the process of SS is initiated. Z. Zhou et al. (2018) [50] present a secret image sharing method based on encrypted pixels and reveals its superiority to permutation-only ciphers. A modified (k, n)-SS scheme has been proposed by them, which is based on Thein and Lin's scheme. In their first approach, they encrypt the secret image using common encryption methods like AES. Then using Thein and Lin's scheme generate small-sized shares. Afterward, the secret key is shared using Shamir's PSS scheme. The key shares are concatenated with the secret share and given to the participants. This increases the size of the shares and is not processing-friendly. To make the size similar to Thein and Lin's scheme, they propose a modified method that embeds the

128-bit key in the encrypted image using a simple XOR operation. However, the security offered by the second approach is not illustrated in detail. The key is not shared using PSS and is recovered from the encrypted image only. If during transmission even one-bit changes, the key value is affected, making the cryptosystem highly sensitive to a one-bit error during transmission.

SS schemes can be (k, n)-based wherein 'k' is the threshold and 'n' is the total number of shares and (2,2)-SS schemes [51]. A (2, 2) threshold scheme has restricted applicability for PHR data storage and distribution. For analysis of (2, 2)-SS schemes, we consider Chen et al.'s (2018) (2, 2) scheme presented in [52]. In their scheme, the secret image is first encrypted using the Henon map, and subsequently, two shares are generated. It can be seen that the proposed method generates shares that are the same size as that of the secret image. Furthermore, the scheme is not fault-tolerant as both the servers are required for the secret image retrieval, and if one gets damaged, the secret data is lost. Similar (2, 2) threshold schemes have been presented in many other research works as well, which lack the flexibility required for PHR storage and distribution. For example, if the patient and doctor already have two shares, the healthcare provider will not gain access to the PHR using these (2, 2)-SS schemes.

3. COMPUTATIONAL SECRET IMAGE SHARING AND ITS ISSUES

In this section, we illustrate the use of CSIS for data security of medical data and discuss its issues. In the PSS scheme, the secret data is divided among a set of 'n' participants, and when a predefined number of them pool their shares together, the secret is revealed back. The sharing polynomial is shown in equation no. 1:

$$f(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_{k-1} x^{k-1} \ mod\ p. \tag{1}$$

The coefficients a_i , *where* a_i *can be* $a_1, \ldots .a_{k-1}$, are random numbers in original (k, n) Shamir's PSS scheme, 'a_0' is the secret to be shared, and 'p' is a large prime number, where p $> a_i$ and p $> a_0$. The value of 'x' is substituted, and a function value is obtained as share, i.e., for i-th share we get $(x_i, f(x_i))$, where$1 \le i \le n$. For secret retrieval, the Lagrange interpolation formula is utilized as shown in equation no. 2:

$$a_0 = f(0) = \sum_{j=1}^{k} y_j \prod_{i \geq 1}^{k} \frac{x_i}{x_i - x_j} \ mod\ p\ x \tag{2}$$

where $'y_j'$ represents the shares of the participants, and $f(0)$ is the secret key. Thein and Lin extended the PSS to secure images. For share generation, Thein and Lin's approach takes the pixel values of the secret image as coefficients of a (k-1)-degree polynomial. The disadvantage of using this scheme is that the shares are far from ideal noise-like images and expose the details of the secret image. The secret image is first permuted as part of the original scheme, and then the sharing process is initiated. However, many subsequent works have presented the vulnerability of permutation-only ciphers against chosen-plaintext attacks. X. Yan et al. (2019) [53] classified four security levels for the SS schemes based on the amount of secret information leakage obtained from an image recovered by (k-1) shares. The security levels for the original Shamir's PSS scheme and Thein and Lin's CSIS scheme are defined as follows:

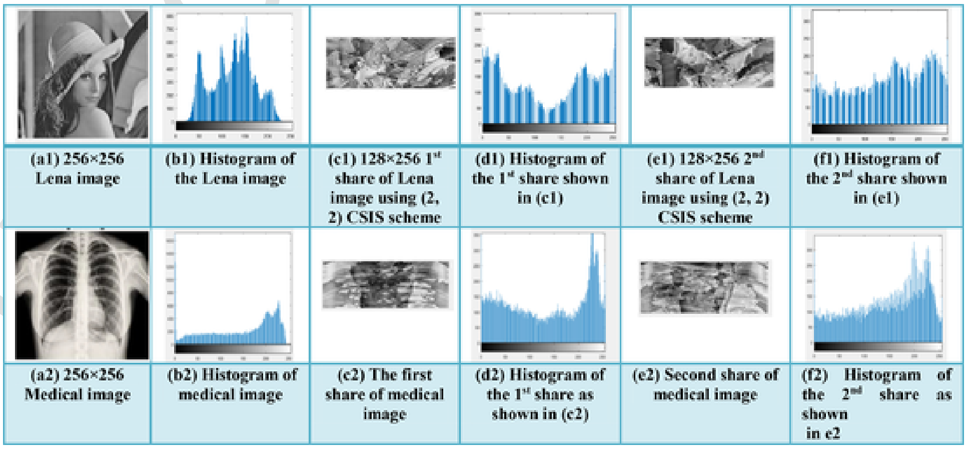
i If $s'_{t<k}$ is the recovered secret pixel from t = k-1 or lesser number of shares, and s is the secret pixel. Then the SS belongs to Level 1 security if $s'_{t<k}$ is random, i.e., Prob $(s'_{t<k} = i) = \frac{1}{p}$ for any pixel value in the range $i \in [0, P-1]$, where 'Prob' represents the probability. It is presented that the original Shamir's (k, n) SS scheme belongs to Level 1 security [53].

ii The SS scheme belongs to Level 3 if$s'_{t<k} = f(s_1)$, where s_1 is the encoded result of$s$. The improved Polynomial-based Thein and Lin's SS belongs to Level 3 security [53]. It is also mentioned that without encoding $s'_{t<k}$ may give a clue about the secret image pixel$s$. Therefore, the encoding technique guarantees security other than the SS itself. If the encoding technique like permutation-only cipher is not strong enough, the resulting cryptosystem will be vulnerable to several attacks.

Fig. 2 represents the shares generated and the corresponding histograms of grayscale Lena image and test medical image. The histogram distributions of the shares are non-uniform, which reveals that the probability of occurrence of some grey levels is more than others. The scheme can be represented as a 'ramp' SS scheme where the exposed secret information is proportional to the number of shares used in the secret recovery process. For security, the secret image has to be encrypted before the SS process is initiated.

4. PROPOSED METHOD

The sustainability of health is an essential paradigm for smart healthcare development. Security techniques have to be employed for medical data in the IoHT-based framework used in smart cities. The medical images that constitute the unstructured form of data in PHRs, can be efficiently stored and distributed using the CSIS scheme on IoHT-based servers. We apply RC6 encryption on the secret images in Cyclic Block Chaining mode (CBC) mode [27]. RC6 can provide a high level of security and flexibility with a lesser number of encryption rounds. It



(a1) 256×256 Lena image

(b1) Histogram of the Lena image

(c1) 128×256 1st share of Lena image using (2, 2) CSIS scheme

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

(e1) 128×256 2nd share of Lena image using (2, 2) CSIS scheme

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

(a2) 256×256 Medical image

(b2) Histogram of medical image

(c2) The first share of medical image

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

(e2) Second share of medical image

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

Fig. 2. (a1, a2) Lena and Medical image. (b1, b2) Histograms of the secret images. (c1, c2, e1, e2) Generated shares using (2, 2) CSIS scheme. (d1, d2, f1, f2) Histograms of the share images.

can be employed with different length keys and is faster than asymmetrical algorithms like RSA. The encrypted image is then converted into multiple shares using the CSIS scheme. The shares are 1/threshold times the size of the secret image and completely hide its contents. The threshold property of the CSIS scheme is maintained, and we cannot obtain any information about the secret image using less than the threshold number of shares. The 128-bit key for RC6 is shared using PSS. The image shares generated are completely noise-like, revealing their strength against various differential and statistical attacks. Furthermore, (k-1) key shares and 'n' image shares can be transmitted publically where 'k' is the threshold, and 'n' is the total number of shares. The remaining ((n-k) + 1) key shares can be secured using the DNA substitution method. Algorithm 1 explains the procedure of share generation for distributed storage and transmission in an IoHT-based system.

The redundancy of the secret data is increased by the threshold scheme, making the system more fault-tolerant. Even if some server crashes or network channels are damaged in the IoHT framework, we can recover the secret data by any 'k' image shares and 'k' key shares. The DNA substitution method, RC6 encryption, and key distribution are described in detail in the following sub-sections. Algorithm 1 uses 257 as the prime number in the sharing polynomial; thus, the shares can have a pixel value equal to 256 [23]. The pixels with a value equal to or more than 255 will be stored in two bytes. For secret reconstruction, if the value of a pixel in the share-image is equal to or more than 255 its's read from two bytes. The first byte will be 255, and the next can be zero or one, which will be added to 255 to get the final value. With the help of this technique, it is possible to recover the secret medical image in a lossless manner.

Medical images are instrumental for the proper diagnosis of a disease, and as such, it is not desirable to use a security technique that degrades the quality of the recovered image to any extent. This forms a major challenge in medical data storage and security by healthcare organizations that have to deliver sustainable care to the citizens of smart cities. When a PHR access request is made to the IoHT-based cloud administrator, it retrieves any 'k' image shares from the cloud servers and performs an inverse CSIS scheme to reconstruct the encrypted image. One key share can be retrieved with the application of inverse DNA substitution on a Stego DNA sequence. The other 'k-1′ key shares can be retrieved from the cloud servers. Application of inverse PSS on these 'k' key shares will recover the secret key used initially for encryption. If a key share is damaged during storage, another Stego DNA sequence can be used to recover a key share permitted by the threshold scheme. The bandwidth and storage requirement of the cryptosystem is also less because the share size is small. Subsequently, RC6 decryption in the CBC mode will be performed to retrieve the secret image in a lossless manner [27].

4.1. RC6 Encryption and Decryption

We will describe in detail all the underlying methods used to ensure the security of the secret images. To encrypt the secret images, we have employed the RC6 encryption technique [54]. RC6 encryption is a well-known symmetric block cipher and is known to be strong against many attacks. It can be applied in the CBC mode to generate noise-like images of fairly uniform histograms and better visual disguise. In CBC mode, XOR operation is performed between the plaintext and a 128-bit key [27]. Then the RC6 algorithm is applied to generate the ciphertext block. The subsequent ciphertext blocks are generated by taking the XOR of the plaintext and the previous ciphertext and application of RC6 encryption. The key used for encryption and XOR operation is the same. During RC6 decryption using CBC mode, all the encryption steps are reversed.

4.2. DNA Substitution and Stego-DNA Sequence

The ((n-k) + 1)) key shares are binary number sequences that can be transmitted by using the DNA substitution table. The bit string is divided into several 2-bit sequences, which are then converted into DNA bases. There are in total four DNA bases called Adenine (A), Guanine (G), Cytosine (C), and Thymine (T). The Stego DNA sequence is generated using a reference DNA sequence from the DNA database. This sequence can then be transmitted via an unsecured channel. For example, if the input sequence is 01 and the reference DNA base is 'A', the transmitted DNA base is 'C' [54, 55]. Similarly, all key-share binary sequences are converted into a string of Stego-DNA sequences. Assume that we have a 2-bit binary key-share sequence as 'M' and a reference DNA base is 'D' then Stego-DNA nucleotide bases can be calculated using the DNA substitution table. This is shown in Table 1.

At the receiver, the original binary number sequence is converted back using the Stego-DNA sequence. The recovery process requires that the transmitter and receiver have access to the same reference DNA sequence. The inverse DNA substitution table is used at the receiver to calculate back the key share as shown in Table 2. If the transmitted DNA sequence is 'C' and the reference DNA sequence is 'A' then the bit pattern retrieved is 01. Assume the Stego-DNA base is D′ and the reference DNA base is D then the 2-bit binary number at the intersection will be the original number that was secured. All of the Stego-DNA bases can be converted back into the binary key share using this method.

4.3. Key Distribution

The secret image will be encrypted using RC6 encryption and a 128-bit binary key. We first divide the 128-bit key into 32 4-bit sub-keys. The 4-bit sub-keys are converted to decimal values. Those decimal values are shared into multiple shares using for example (4, 5) Shamir's PSS scheme. The (4, 5) scheme is used for illustration, and any other (k, n) PSS scheme can also be utilized. In this scheme, the secret is the constant term of a (k-1)-degree polynomial. The key is the decimal equivalent of the 4-bit binary sub-key. The generated shares for the first decimal sub-key have a range of more than 16 (2^4). Therefore we require 5 bits to represent the first key share, 6-bits to represent the 2nd key share, 7-bits to represent the 3rd key share, and 8-bits to represent the 4th key share in a (4, 5)-PSS scheme. The 32 (128-bit = 32 × 4) sub-keys are shared using Shamir's sharing polynomial with only the constant term being changed, and coefficients are chosen randomly. The generated shares are converted into binary forms for transmission. The first key share is of 160-bit length (32 × 5), the second key share is of 192-bit length (32 × 6), the third key share is 224-bit (32 × 7), and the fourth

Table 1
Stego DNA base (D') generated using a DNA substitution table with the help of a reference DNA base (D) and key-share (M). Nucleotide bases Adenine (A), Guanine (G), Cytosine (C), and Thymine (T) are used.

D→ M↓	A	C	T	G
00	A	C	T	G
01	C	T	G	A
10	T	G	A	C
11	G	A	C	T

Table 2
Inverse DNA substitution at the receiver using Stego-DNA base D' and reference DNA base D. Nucleotide base Adenine (A) Guanine (G), Cytosine (C), and Thymine (T) are used.

D→ D'↓	A	C	T	G
A	00	11	10	01
C	01	00	11	10
T	10	01	00	11
G	11	10	01	00

key share is 256-bit (32 × 8). As the number of shares increases, the key-share length also increases. These (k-1) binary key-shares can be publically transmitted, and the remaining ((n-k) + 1) binary key-shares are secured using the DNA substitution method, which requires a reference DNA sequence. This process is summarized in Algorithm 3 and is further illustrated by Example 1, as shown below.

Example 1: Illustration of the process of a key distribution represented in Algorithm 3 using (4, 5)-PSS scheme. Assume a 128-bit key sequence used for RC6 encryption as shown below.

0101000010001000000000001100010010000011000010000100 0010100010110000001100100110000000100000010011000000010 000000010110000100000

Step 1 and 2 of Algorithm 3 Convert the binary sequence into 32 decimal sub-keys taking 4-bits at a time.

0101 0000 1000 1000 0000 0000 1100 0100 1000 0011 0000 1000 0100 0010 1000 1011 0000 0011 0010 0110 0000 0010 0000 0100 1100 0000 0100 0000 0010 1100 0010 0000

The decimal sub-keys are shown below. It is seen that 0101 is equal to 5 in decimal, 0000 is equal to 0, and 1000 is 8. Similarly, all the 4-bit binary numbers are converted into decimal numbers.

5 0 8 8 0 0 12 4 8 3 0 8 4 2 8 11 0 3 2 6 0 2 0 4 12 0 4 0 2 12 2 0

Step 3 of Algorithm 3 Use one decimal sub-key at a time to generate 5 decimal share values using a sharing polynomial. The coefficients of this polynomial are random numbers. For illustration, we take a = 2, b = 1, and c = 3 randomly, and 'S' is the decimal sub-key taken one at a time. Here 4 is the threshold of the scheme as such, we need a 3rd-degree polynomial which is shown below in equation no. 5.

$$\begin{aligned} &For\ (4,5) - PSS\ scheme\ use\ the\ polynomial\ f(x) \\ &= S + 3x + x^2 + 2x^3\ mod\ 257. \end{aligned} \tag{3}$$

Each server is assigned an identity value that is substituted into the sharing polynomial to generate a key share. In this example, we have generated 5 shares, but only 4 are required for secret reconstruction. The secret 'S' will be iteratively replaced by a decimal sub-key for share generation; this is shown in Table 3 (5th share not shown).

Step 4 and 5 in Algorithm 3 Convert each share into binary number taking 5-bits, 6-bits, 7-bits, and 8-bits for the 1st, 2nd, 3rd, and 4th share, respectively. The (k-1) key shares are transmitted publically. Key Share 1 is 32 × 5 = 160-bit binary sequence. Key Share 2 is 32 × 6 = 192-bit binary sequence. Key Share 3 is 32 × 7 = 224-bit binary sequence. Key Share 4 is 32 × 8 = 256-bit binary sequence. For remaining ((n-k) + 1) key-shares the binary sequence is converted into a Stego-DNA sequence using the substitution table.

For reconstruction, the Stego-DNA is converted back into the binary sequence using inverse DNA substitution. The secret key is recovered back using inverse PSS, which is illustrated as follows:

Share no. 1: For the 160-bit binary sequence generated as '01011 00110 01110...' combine 5-bits at a time to form decimal values 11, 6, 14, 14, and so on.

Table 3
Key shares generated by the PSS scheme using the sharing polynomial in Eq. 5.

Shares generated using PSS	Key Share 1 k_1	Key Share 2 k_2	Key Share 3 k_3	Key Share 4 k_4
Secret term S is equal to 5	11	31	77	161
Secret term S is equal to 0	6	26	72	156
Secret term S is equal to 8	14	34	80	164
	⋮	⋮	⋮	⋮
32nd decimal sub-key. Secret term S is equal to 0	6	26	72	156

Share no. 2: For the 192-bit binary sequence '011111 011010 100010100010 ...' combine 6-bits at a time to form decimal values 31, 26, 34, 26, and so on.

Using 4 linear equations no. 6, 7, 8, and 9, having identity values, i.e., x values as 1, 2, 3, and 4 and polynomial values as 11, 31, 77, and 161, first decimal sub-key equal to '5′ can be recovered:

$$a + b + c + d = 11 \tag{4}$$

$$8a + 4b + 2c + d = 31 \tag{5}$$

$$27a + 9b + 3c + d = 77 \tag{6}$$

$$64a + 16b + 4c + d = 161x \tag{7}$$

The solution a = 2, b = 1, c = 3 (random coefficients of sharing polynomial), and d = 5 (First decimal secret sub-key) can be revealed. The same procedure is used to get the 32 sub-keys (5 0 8 8... so on.) and converted to a 128-bit binary sequence (0101 0000 1000 1000 0000....so on) using 4-bit representation. This is the same 128-bit key used for RC6 encryption. Using this key, the recovered secret image is decrypted.

5. RESULTS AND DISCUSSION

To evaluate the proposed method, several experiments have been conducted on the grayscale test images. The experiments were conducted on Windows 10 Operating system using MATLAB R2017a (version 9.2.0 538062). The modules developed in MATLAB can be deployed in the IoHT framework using the MATLAB runtime/MATLAB coder that can generate stand-alone executable files and C/C++ code for embedded systems. For encryption and SS, test images are resized to 256 × 256. The test images are first encrypted using RC6 encryption. The encrypted image is then shared using the (2, 2) Thein and Lin' CSIS scheme to observe the share image quality. However, the number of shares can be increased to any value, creating room for more participants in the SS process. This is an advantage over the (2, 2) schemes, which are not fault resistant. The computational overhead increases by using RC6 encryption and a 128-bit key-value, respectively, need to be shared. For all comparisons with shares, the original secret image is resized to 128 × 256. The medical images have been taken from the OPENi medical image database, as shown in Fig. 3. For illustration purposes, several natural test images are also taken for the experiments.

5.1. Encryption Evaluation Metrics

The encryption algorithm must hide the contents of the secret image completely and should be able to withstand many attacks. These attacks include brute-force, statistical, and differential attacks, among others. The SS and encryption should generate shares with the following characteristics:

i **Uniform Histogram**

Histograms of the shares generated by the CSIS scheme with RC6 encryption are fairly uniform as shown in Fig 4. The histogram $h(r_k)$of an image is given by the following mathematical equation no. 10:

$$h(r_k) = n_k \tag{8}$$

Where r_k is the kth intensity value and n_k represents the number of pixels in the image having an intensity equal to r_k.

i **The low value of the correlation between the secret image, encrypted image, secret shares, and infinite PSNR**

The correlation represents a measure of randomness of the intensity values in the shares. The correlation C, as shown in equation no. 11,

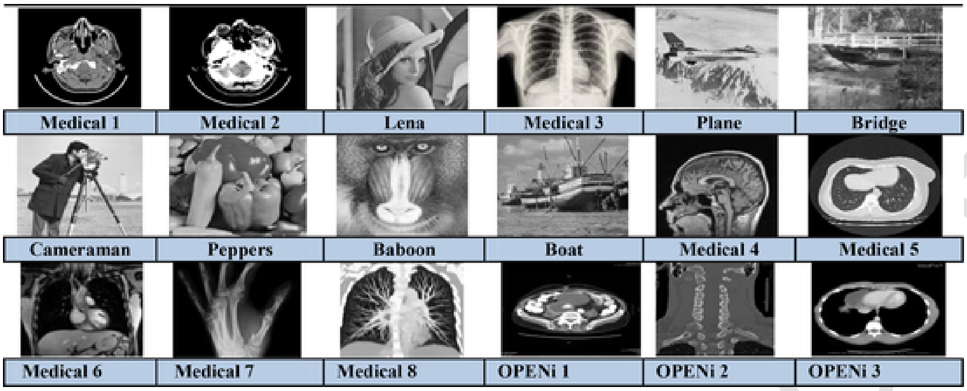


Fig. 3. Examples of Test images (Source for medical Images: OPENi Medical Image Database available at https://openi.nlm.nih.gov/index.php/).

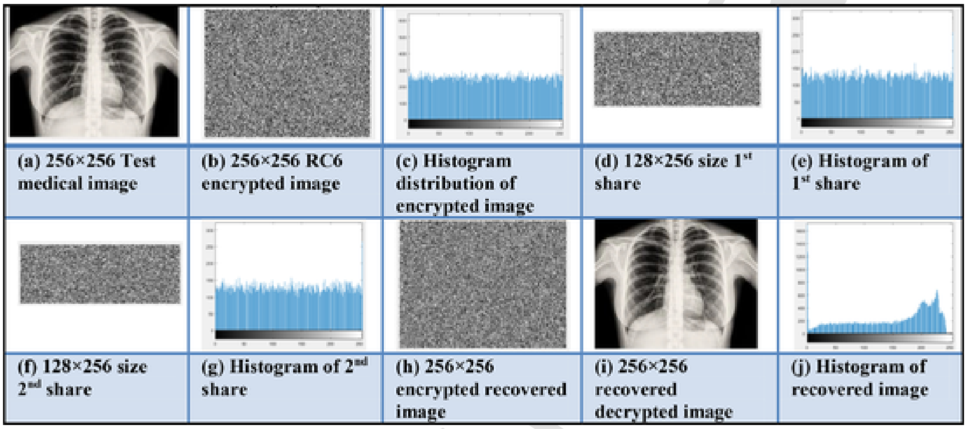

(a) 256×256 Test medical image
(b) 256×256 RC6 encrypted image
(c) Histogram distribution of encrypted image
(d) 128×256 size 1st share
(e) Histogram of 1st share
(f) 128×256 size 2nd share
(g) Histogram of 2nd share
(h) 256×256 encrypted recovered image
(i) 256×256 recovered decrypted image
(j) Histogram of recovered image

Fig. 4. Thein and Lin's (2, 2) CSIS with RC6 encryption of test medical image. (a) 256 × 256 Medical image. (b) 256 × 256 RC6 encrypted image. (c) Histogram of the encrypted image. (d-g) 128 × 256 sized shares and histogram. (h) Recovered encrypted image. (i, j) 256 × 256 Lossless recovered decrypted image and its histogram.

should be +1 and PSNR, as shown in equation no. 12, should be equal to ∞ for the original secret image I (i, j) and recovered secret image I′(i, j) as in Fig. 5. The correlation and PSNR values of the secret image and recovered image are shown in Table 4.

$$C = \frac{n\left(\sum xy\right) - \left(\sum x\right)\left(\sum y\right)}{\sqrt{n\sum x^2 \;--\left(\sum x\right)^2\left[n\sum y^2 \;--\left(\sum y\right)^2\right]}} \tag{9}$$

$$PSNR = 20 \times \log_{10}\left(\frac{(255)^2}{\sqrt{MSE}}\right) dB \tag{10}$$

Where $MSE = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}\left(I\,(i,j) - I'\,(i,j)\right)^2$

i Better Visual Disguise

The shares generated by the CSIS scheme with RC6 encryption are random images that do not reveal any information about the secret image hence improving the residual image problem and security factor. This is shown in Fig. 4.

Continue4i Better Diffusion Characteristics

To evaluate the diffusion characteristics, we use the parameter called NPCR, as shown in Table 5. In the proposed method, all the share images have NPCR values of more than 99.50%. Let S1 (i, j) represent the first share image, and S2 (i, j) represents the 1st share image when the input image is changed by 1 bit to calculate NPCR1 using equation no. 13. Similarly, NPCR2 will be calculated between the 2nd share image and the 2nd share image generated by changing the secret image by 1-bit using the same equation no. 13. The comparison of NPCR values with state-of-the-art schemes is shown in Table 6.

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

$$NPCR1\,(S1,S2) = \sum i,j\ \frac{D\,(i,j)}{M \times N} \times 100\% \ \ (13)$$

Continue4i Key-Space Analysis

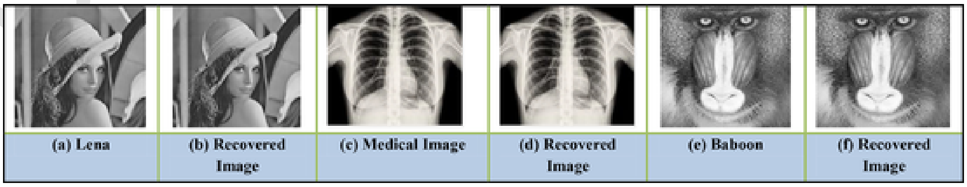

(a) Lena
(b) Recovered Image
(c) Medical Image
(d) Recovered Image
(e) Baboon
(f) Recovered Image

Fig. 5. Lossless recovery of grayscale secret images for the proposed scheme.

Table 4
PSNR and Correlation between the secret and recovered images.

Secret images and Lossless recovered image	Correlation	PSNR in dB
Fig. 5(a), (b) Lena, Recovered Lena image	1	∞
Fig. 5(c), (d) Medical Image, Recovered Medical Image	1	∞
Fig. 5(e), (f) Baboon, Recovered Baboon image	1	∞

Table 5
NPCR values between two shares for RC6-CSIS.

Test images encrypted using RC6 encryption with (2,2)-CSIS	NPCR1 (%) between 1st share images	NPCR2 (%) between 2nd share images
Medical 1	99.62	99.63
Medical 2	99.58	99.63
Medical 3	99.54	99.60
Lena	99.61	99.62
Baboon	99.56	99.58
Bridge	99.57	99.62
Cameraman	99.63	99.62
Peppers	99.65	99.64
Plane	99.61	99.62
Boat Image	99.58	99.59
Medical 4	99.58	99.62
Medical 5	99.66	99.53
Medical 6	99.61	99.64
Medical 7	99.64	99.59
Medical 8	99.63	99.59
OPENi 1	99.64	99.60
OPENi 2	99.63	99.62
OPENi 3	99.64	99.60

Table 6
Comparison of NPCR with state-of-the-art schemes.

Image	NPCR1 between 1st share	NPCR2 between 2nd share	[56]	[57]	[58]	[59]	[61]
Lena	99.61	99.62	99.62	99.61	99.62	99.60	99.59
Baboon	99.56	99.58	-	-	-	-	99.61
Cameraman	99.63	99.62	-	99.60	-	-	99.60

The sensitivity to cipher keys is a good parameter to evaluate the strength of a cryptosystem. For the RC6 encryption scheme, a 128-bit key is used, which can be predicted if all 2^{128} possible combinations are attempted one after the other, which is infeasible to perform. Hence the cryptosystem is strong against brute-force attacks.

Continue4i **Information Entropy**

Entropy H(R) of source R is shown in equation no. 14.

Table 7
Entropy and SSIM values for shares.

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
Medical 1	7.9919	7.9918	0.0015	0.0005
Medical 2	7.9921	7.9927	0.0021	0.0032
Medical 3	7.9920	7.9925	0.0078	0.0078
Lena	7.9922	7.9931	0.0073	0.0079
Baboon	7.9934	7.9917	0.0082	0.0088
Bridge	7.9926	7.9914	0.0102	0.0102
Peppers	7.9920	7.9924	0.0094	0.0115

Table 8
Comparison of entropy values with recent schemes.

Images	The entropy of 1st share	The entropy of 2nd share	[56]	[60]	[61]	[62]
Lena	7.9922	7.9931	7.9975	7.9894	7.9974	7.9983
Baboon	7.9934	7.9917	-	-	7.9968	-

$$H(R) = \sum_{i=0}^{M-1} Prob\left(R_i\right) \log \frac{1}{\left(R_i\right)} \tag{11}$$

Where M represents the total symbols $\mathbf{R_i} \in \mathbf{R}$, and entropy is represented in bits. It is an effective parameter to measure the randomness of encrypted images and generated shares. For both the shares of secret images, we see that the information entropy is more than 7.99, which reveals that the system is secure against entropy attacks, as shown in Table 7, and the comparison is shown in Table 8.

Continue4i **SSIM**

SSIM is used to calculate the image structural similarity. In Table 7, we have also indicated the SSIM value between the secret image and the share images that are very close to zero.

Continue4i **Comparative** Analysis of Related SS Methods

The survey of different SS schemes was conducted, as shown in Table 9. It represents the differences of our proposed method with other SS schemes in terms of fault tolerance, lossless recovery, shares size, etc.

Continue4i **Issues** and Future Research

There are many advantages of using Thein and Lin's approach to share generation, as mentioned earlier. By conducting a detailed survey of different SS schemes like VSS, (2, 2)-Boolean-

Table 9
Comparative analysis of the proposed scheme with related schemes.

Property	Shamir's Scheme [48]	Thein and Lin's Scheme [44]	X. Zhou et al. [49]	VSS [51]	Chen et. al.'s Scheme [52]	Proposed Scheme
Fault Tolerance	Yes	Yes	Yes	Yes	No	Yes
Threshold Property	Yes	Yes	Yes	Yes	No	Yes
Share Size	Same as secret image	(1/k) times secret image	(1/(k-1)) times the secret image.	Bigger than the secret image (Pixel Expansion)	Same as secret image	≥(1/k) times secret image
Lossless Recovery	No	No	Yes	No	Yes	Yes
Transmission Time	More	Less	Less	More	More	Less
Encryption/ Permutation	No	Permutation	Arnold Permutation	No	Henon Map Permutation	RC6 encryption

Algorithm 1
Thein and Lin's CSIS with RC6 encryption (Enc).

```
Input: Grayscale M × N secret image, encryption key, (k, n) parameters, suitable
prime number p

Step 1: Encrypt the secret image S to get S′
  S′← Enc (S)
  Step 2: Generate blocks of the encrypted image
  $B_0, B_{1\ldots} B_{k-1}$← Blocking (S′)
  Where k is the number of pixels in each block.
  Step 3: Generate a (k-1)-degree polynomial for every block represented as:
  $f(x) = a_0 + a_1x + a_2x^2 + \ldots + a_{k-1}x^{k-1}$ m
      od 257. (3)
  In which $a_i = B_i,\ i = 0, 1, 2, \ldots k-1$.
  Step 4: Calculate
  $SC_1 = f(1), SC_2 = f(2) \ldots\ldots SC_n = f(n)$.
  Step 5: Arrange $SC_1$ to $SC_1$(i, j), $SC_2$ to $SC_2$(i, j) ..., $SC_n$ to $SC_n$ (i, j)
  Step 6: Repeat Steps 2-5 for all pixels of S′
  Step 7: Output the 'n' share images $SC_1$, $SC_2$, ..., $SC_n$
  Step 8: Divide the 'b'-bit key 'K' into 4-bit sub-keys.
  Step 9: Generate a 3rd-degree polynomial for (4,5)-PSS scheme.
  $f(x) = a_0 + a_1x + a_2x^2 + a_3x^3 \bmod 257$. (4)
  where '$a_0$' is the decimal sub-key.
  Step 10: Generate the key-shares $k_1, k_{2\ldots} k_n$ mod 257 for each sub-key using PSS.
  Step 11: Transmit the sub-keys $k_1, k_{2\ldots} k_{k-1}$, and share images $SC_1$, $SC_2$, ..., $SC_n$
  publically and secure the remaining keys using a simple DNA substitution
  algorithm to generate Stego-DNA sequences.
Output: 'n' Image shares, 'k-1' key shares and ((n-k) + 1) Stego-DNA sequences.
```

Algorithm 2
describes the secret reconstruction process in detail.

Algorithm 2: *Thein and Lin's computational secret image reconstruction and RC6 decryption (Dec)*

```
Input: One Stego-DNA sequence, k Image Shares, (k-1) key-shares, (k, n)
  parameters, suitable prime number p
Step 1: Take any one Stego-DNA sequence and apply inverse DNA substitution to
  extract the key share.
  Step 2: Generate the key bits using the inverse PSS scheme.
  K = $PSS^{-1}$ ($k_1, k_{2\ldots} k_k$)
  Step 3: Take $SC_1$, $SC_2 \ldots SC_k$ image shares and applies the reconstruction process
  by solving linear equations to generate the reconstructed, encrypted image.
  S′ = $CSIS^{-1}$ ($SC_1$, $SC_2 \ldots SC_k$)
  Step 4: By providing the key, decrypt the original secret image.
  S = Dec (S′)
  Step 5: Output the Grayscale M × N secret image S.
Output: Grayscale M × N secret image S
```

Algorithm 3
Key Distribution.

```
Input: The 128-bit key used for RC6 encryption.

Step 1: Divide the key into 32 4-bit sub-keys
  Step 2: The 4-bit sub-keys are converted to decimal values
  Step 3: Those decimal values are shared using (4, 5)-PSS scheme, where k = 4
  and n = 5.
  Step 4: Convert them into binary form. The (k-1) key shares i.e., 3 shares can be
  publically transmitted
  Step 5: Remaining ((n-k) + 1) = 2 shares are secured using the DNA substitution
  method, which requires a reference DNA sequence.
Output: (k-1) key shares, ((n-k) + 1) key shares for subsequent DNA substitution.
```

based SS, and Shamir's PSS scheme, we conclude that the proposed technique has the advantages of fault tolerance and reduced share size. The residual image problem is mitigated using the RC6 encryption method. The encryption key is shared using the PSS scheme, which provides perfect security. However, there are many challenges in the implementation of the cryptosystem, which are enlisted as follows:

- The scheme utilizes RC6 encryption with CSIS and, as such, has high computational complexity.
- The shares generated are not noise-resistant.
- The proposed framework employs Lossless CSIS by making use of a prime number equal to 257. Therefore, for the pixels in the share with a value that is more than 255, 2-bytes of information needs to be stored.

Many improvements to the existing cryptosystem are required to be utilized effectively in smart, sustainable cities. The most important factors are the reduction in secret recovery time and computational complexity. This could be realized by using alternative methods to solving a linear system of equations. Attention also needs to be given to the robustness of the cryptosystem towards the noise.

CONCLUSION

A smart city aims to improve sustainability with the help of technological automation. Millions of PHRs are created because of the use of IoHT in smart cities. The CSIS method can be efficiently used to distribute the unstructured data of PHRs in the IoHT-based platforms. In this work, we try to overcome the residual image problem by applying the RC6 encryption technique. Afterwards, this encrypted image is converted into secret shares using the CSIS scheme. The secret key is also shared using PSS. We demonstrate that 'n' image shares and (k-1) key shares can be transmitted or stored publically. The remaining ((n-k) + 1)) key shares are secured using a DNA substitution algorithm. The DNA substitution method requires the use of a reference DNA sequence. The entropy of the generated shares is more than 7.99, and SSIM values are negligible. The NPCR values are more than 99.55% for all the shares that show a high diffusion measure. In the future, we intend on improving the other issues with the CSIS scheme that include reduction of computational complexity, fast secret recovery, and generation of noise-resistant shares. Another research direction can be to develop faster and more efficient encryption schemes for CSIS.

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.

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. This work was also supported by the National Research Foundation of Korea (NRF) grant funded by the Korean government (MSIP) (No.2016R1A2B4011712).

Acknowledgment

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.

References

Yigitcanlar, T., Kamruzzaman, M., Foth, M., Marques, J. S., da Costa, E., & Ioppolo, G. (2019). *Can cities become smart without being sustainable? A systematic review of the literature. Sustainable cities and societies, 45*, 348–365.

Shorfuzzaman, M., Hossain, M. S., & Alhamid, M. F. (2021). *Towards the sustainable development of smart cities through mass video surveillance: A response to the COVID-19 pandemic. Sustainable Cities and Society, 64*.

Palozzi, G., Binci, D., & Schettini, I. (2020). Digital Transformation in the Healthcare Sector: Empirical Evidences of IoHT Benefits and Limits on Chronic Disease Management. In D., Cagáňová, & N., Horňáková (Eds.), *Mobility Internet of Things. Mobility IoT 2018. EAI/Springer Innovations in Communication and Computing*. Springer.

Mukherjee, S. G., Behere, A., et al. (2021). *Internet of Health Things (IoHT) for personalized health care using an integrated edge-fog-cloud network. J Ambient Intell Human Comput, 12*, 943–959.

Rathore, M. M., Paul, A., Hong, W. H., Seo, H. C., Awan, I., & Saeed, S. (2018). *Exploiting IoT and big data analytics: Defining Smart Digital City using real-time urban data. Sustainable Cities and Society*, *40*, 600–610.

Kaw, J. A., Loan, N. A., Parah, S. A., Muhammad, K., Sheikh, J. A., & Bhat, G. M. (2019). *A reversible and secure patient information hiding system for IoT driven e-health. International Journal of Information Management*, *45*, 262–275.

Kim, H. M., et al. (2021). *Smart cities as a platform for technological and social innovation in productivity, sustainability, and livability: A conceptual framework. Smart Cities for Technological and Social Innovation*, *9*(28).

Badawi, H. F., & El Saddik, A. (2020). *Biofeedback in Healthcare: State of the Art and Meta-Review* A. El Saddik, M. Hossain, B. Kantarci. *Connected Health in Smart Cities*. Cham: Springer.

Muhammad, G., Hossain, M. S., & Yassine, A. (2020). *Tree-Based Deep Networks for Edge Devices. IEEE Transactions on Industrial Informatics*, *16*(3), 2022–2028.

Muhammad, G., Alhamid, M. F., & Long, X. (2019). *Computing and Processing on the Edge: Smart Pathology Detection for Connected Healthcare. IEEE Network*, *33*(6), 44–49.

Liu, J., et al. (2020). *Recent Advances of Image Steganography with Generative Adversarial Networks. IEEE Access*, *8*, 60575–60597.

Parah, S. A., Sheikh, J. A., Akhoon, J. A., & Loan, N. A. (2020). *Electronic Health Record hiding in Images for smart city applications: A computationally efficient and reversible information hiding technique for secure communication. Future Generation Computer Systems*, *108*, 935–949.

Muhammad, K., Hamza, R., Ahmad, J., Lloret, J., Wang, H., & Baik, S. W. (2018). *Secure Surveillance Framework for IoT systems using Probabilistic Image Encryption. IEEE Transactions on Industrial Informatics*, *14*, 3679–3689.

Basit, A. and A. (2019). An Extended Protected Secret Sharing Scheme. *2019 International Conference on Electrical, Electronics and Computer Engineering (UPCON)* (pp. 1–4).

Sun, Y., Lu, Y., Chen, J., Zhang, W., & Yan, X. (2020). *Meaningful Secret Image Sharing Scheme with High Visual Quality Based on Natural Steganography. Mathematics*, *8*(9), 1452.

Bibri, S. E. (2018). *The IoT for smart sustainable cities of the future: An analytical framework for sensor-based big data applications for environmental sustainability. Sustainable Cities and Society*, *38*, 230–253.

Zhang, L., Ye, Y., & Mu, Y. (2021). *Multi authority Access Control with Anonymous Authentication for Personal Health Record. IEEE Internet of Things Journal*, *8*(1), 156–167.

Edemacu, K., Jang, B., & Kim, J. W. (2020). *Efficient and Expressive Access Control with Revocation for Privacy of PHR Based on OBDD Access Structure. IEEE Access*, *8*, 18546–18557.

Sandhu, R., Gill, H. K., & Sood, S. K. (2016). *Smart monitoring and controlling of Pandemic Influenza A (H1N1) using Social Network Analysis and cloud computing. Journal of Computational Science*, *Vol.12*, 11–22.

Butpheng, C., Yeh, K. H., & Xiong, H. (2020). *Security and Privacy in IoT-Cloud-Based e-Health Systems—A Comprehensive Review. Symmetry*, *12*(7), 1191.

Iqbal, F. U., Anwar, H., Kwak, K. S., Imran, M., Jamal, W., & Rahman, A. (2018). *Interoperable Internet-of-Things platform for a smart home system using Web-of-Objects and cloud. Sustainable Cities and Society*, *38*, 636–646.

Ullah, F., Habib, M. A., Farhan, M., Khalid, S., Durrani, M. Y., & Jabbar, S. (2017). *Semantic interoperability for big-data in heterogeneous IoT infrastructure for healthcare. Sustainable Cities and Society*, *34*, 90–96.

Wang, S. (2020). *Distributed Storage based on Secret Sharing Schemes (D4S). MATLAB Central File Exchange. Retrieved March*, *29*.

Nooh, S. A. (2020). Cloud Cryptography: User End Encryption. *2020 International Conference on Computing and Information Technology (ICCIT-1441)* (pp. 1–4).

Wang, X., & Liu, L. (2020). *Image Encryption Based on Hash Table Scrambling and DNA Substitution. IEEE Access*, *8*, 68533–68547.

Meier, W., & Knudsen, L. R. (2000). Correlations in RC6 with a Reduced Number of Rounds Source. *Proceedings of the 7th International Workshop on Fast Software Encryption* (pp. 94–108).

El-Samie, F. E. A. (2014). *Image Encryption A Communication Perspective*. CRC Press, Taylor & Francis Group.

Hu, W. W., Zhou, R. G., Jiang, S., et al. (2020). *Quantum image encryption algorithm based on generalized Arnold transform and Logistic map. CCF Trans. HPC*, *2*, 228–253.

Silva, D. A., Verducci, O., & Oliveira, D. L. (2019). Implementation of DES Algorithm in New Non-Synchronous Architecture Aiming DPA Robustness. *2019 IFIP/IEEE 27th International Conference on Very Large-Scale Integration (VLSI-SoC)* (pp. 228–229).

Kaur, G., Agarwal, R., & Patidar, V. (2020). *Chaos-based multiple order optical transforms for 2D image encryption. Engineering Science and Technology, an International Journal*, *23*(5), 998–1014.

Patro, K. A. K., Soni, A., Netam, P. K., & Acharya, B. (2020). *Multiple grayscale image encryption using cross-coupled chaotic maps. Journal of Information Security and Applications*, *52*.

Silva, B. N., Khan, M., & Han, K. (2018). *Towards sustainable smart cities: A review of trends, architectures, components, and open challenges in smart cities. Sustainable Cities and Society*, *38*, 697–713.

Muhammad, G., Alhamid, M. F., Alsulaiman, M., & Gupta, B. (April 2018). *Edge Computing with Cloud for Voice Disorders Assessment and Treatment. IEEE Communications Magazine*, *56*(4), 60–65.

Dagher, G. G., Mohler, J., Milojkovic, M., & Marella, P. B. (2018). *Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology. Sustainable Cities and Society*, *39*, 283–297.

Wang, X., & Liu, C. (2017). *A novel and effective image encryption algorithm based on chaos and DNA encoding. Multimed Tools Appl*, *76*, 6229–6245.

Wang, X., Li, P., Qian, Y., Liu, L., Zhang, H., & Wang, X. (2018). *A novel color image encryption scheme using DNA permutation based on the Lorenz system. Multimed Tools Appl*, *77*, 6243–6265.

Wu, X., Wang, K., Wang, X., Kan, H., & Kurths, J. (2018). *Color image DNA encryption using NCA map-based CML and one-time keys. Signal Processing*, *148*, 272–287.

Wu, J., Liao, X., & Yang, B. (2018). *Image encryption using 2D Henon-Sine map and DNA approach. Signal Processing*, *153*, 11–23.

Rehman, X. L. (2019). *A novel robust dual diffusion/confusion encryption technique for color image based on Chaos, DNA and SHA-2. Multimed Tools Appl*, *78*, 2105–2133.

Zhu, S., & Zhu, C. (2020). *Secure Image Encryption Algorithm Based on Hyper-chaos and Dynamic DNA Coding. Entropy*, *22*(7), 772.

Jithin, K. C., & Sankar, S. (2020). *Colour image encryption algorithm combining Arnold map, DNA sequence operation, and a Mandelbrot set. Journal of Information Security and Applications*, *50*.

Gutub, N. A.-J., & Khan, E. (2019). *Counting-based secret sharing technique for multimedia applications. Multimed Tools Appl*, *78*, 5591–5619.

Gutub, M. A.-G. (2020). *Hiding shares by multimedia image steganography for optimized counting-based secret sharing. Multimed Tools Appl*, *79*, 7951–7985.

Thien, C., & Lin, J. C. (2003). *An Image-Sharing Method with User-Friendly Shadow Images. IEEE Transactions on Circuits and Systems for Video Technology*, *13*(12), 1161–1169.

Wu, K. S. (2013). *A secret image sharing scheme for light images. EURASIP J. Adv. Signal Process.*, *49*, 2–5.

Jolfaei, X. W. W., & Muthukkumarasamy, V. (2016). *On the security of Permutation-Only Image Encryption Schemes. IEEE Trans. Inf. Forensics Security*, *11*(2), 235–246.

Xie, L. L., Peng, H., & Yang, Y. (2017). *A Secure and Efficient Scalable Secret Image Sharing Scheme with Flexible Shadow Sizes. PLoS ONE*, *12*.

Ding, W., Liu, K., Yan, X., & Liu, L. (2018). *Polynomial-Based Secret Image Sharing Scheme with fully lossless Recovery. Int J. Digit. Crime Forens. IJDCF*, *10*, 120–136.

Zhou, X., Lu, Y., Yan, X., Wang, Y., & Liu, L. (2018). *Lossless and Efficient Polynomial-Based Secret Image Sharing with Reduced Shadow Size. Symmetry*, *10*.

Zhou, Z., Yang, C., Cao, Y., & Sun, X. (2018). *Secret Image Sharing Based on Encrypted Pixels. IEEE Access*, *6*, 15021–15025.

Hu, H., Shen, G., Liu, Y., Fu, Z., & Yu, B. (2018). *Improved schemes for visual secret sharing based on random grids. Multimedia Tools and Applications.* https://doi.org/10.1007/s11042-018-6738-2.

Chen, Y., Lin, J. Y., Chang, C. C., & Hu, Y. C. (2018). *Sharing a Secret Image in the Cloud using Two Shadows. International Journal of Network Security*, 1.

Yan, X., Liu, L., Lu, Y., & Gong, Q. (2019). *Security analysis and classification of image secret sharing. Journal of Information Security and Applications*, *47*, 208–216.

Islam, M. A., Sarker, M. S., Hossen, M. S., Hasan Mridul, A., Hasib, M. A., & Jabiullah, M. I. (2020). A Multi-layer Cryptosystem for Secure Data Transmission using PRNG. *2020 3rd International Conference on Intelligent Sustainable Systems (ICISS)* (pp. 1189–1196).

Khan, J. S., et al. (2020). *DNA and Plaintext Dependent Chaotic Visual Selective Image Encryption. IEEE Access*, *8*, 159732–159744.

Chai, X., Zhang, J., Gan, Z., et al. (2019). *Medical image encryption algorithm based on Latin square and memristive chaotic system. Multimedia Tools and Applications*, *78*, 35419–35453.

Xu, L., Gou, X., Li, Z., & Li, J. (2017). *A novel chaotic image encryption algorithm using block scrambling and dynamic index-based diffusion. Optics and Lasers in Engineering*, *91*, 41–52.

Fang, P., Liu, H., Wu, C., & Liu, M. (2021). *A Secure Chaotic Block Image Encryption Algorithm Using Generative Adversarial Networks and DNA Sequence Coding. Mathematical Problems in Engineering.* https://doi.org/10.1155/2021/6691547.

Askar, S. S., Karawia, A. A., Al-Khedhairi, A., & Al-Ammar, F. S. (2019). *An Algorithm of Image Encryption Using Logistic and Two-Dimensional Chaotic Economic Maps. Entropy*, *21* (44).

Li, T., Du, B., & Liang, X. (2020). *Image Encryption Algorithm Based on Logistic and Two-Dimensional Lorenz. IEEE Access*, *8*, 13792–13805.

Wan, Y., Gu, S., & Du, B. (2020). *A New Image Encryption Algorithm Based on Composite Chaos and Hyperchaos combined with DNA Coding. Entropy*, *22*(2), 171.

An, F. P., & Liu, J. E. (2019). *Image encryption algorithm based on adaptive wavelet chaos. J. Sensors*, *2019*, 1–12.