IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received July 7, 2021, accepted July 16, 2021, date of publication July 21, 2021, date of current version August 3, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3099004

Cryptanalysis of Internet of Health Things Encryption Scheme Based on Chaotic Maps

NOOR MUNIR[1], MAJID KHAN[1], MOHAMMAD MAZYAD HAZZAZI[2], AMER ALJAEDI[3], ABD AL KARIM HAJ ISMAIL[4,5], ADEL R. ALHARBI[3], AND IQTADAR HUSSAIN[6]

[1]Department of Applied Mathematics and Statistics, Institute of Space Technology, Islamabad 44000, Pakistan
[2]Department of Mathematics, College of Sciences, King Khalid University, Abha 61413, Saudi Arabia
[3]College of Computing and Information Technology, University of Tabuk, Tabuk 71491, Saudi Arabia
[4]Department of Mathematics and Sciences, Ajman University, Ajman, United Arab Emirates
[5]Nonlinear Dynamics Research Center (NDRC), Ajman University, Ajman, United Arab Emirates
[6]Department of Mathematics, Statistics and Physics, Qatar University, Doha, Qatar

Corresponding author: Majid Khan (mk.cfd1@gmail.com)

This work was supported by the Deanship of Scientific Research at King Khalid University through the Research Groups Program under Grant R. G. P. 2/150/42.

ABSTRACT Many encryption algorithms are designed to decrease the probability of cyberattacks by assuring data security as well as system and participant authentication. However, in the development of computer resources cryptanalytical techniques have been developed and performed competitively in information security with good results. In this paper, we reported security flaws in the recently offered encryption technique based on a chaotic map for Internet of Health Things (IoHT) security. The scheme was based on a new chaotic map, modified Mandelbrot set, and conditional shift algorithm asserting the encryption algorithm is secure. We have performed some cryptographic attacks to retrieve the key from the understudy cryptosystem. The key was retrieved in little computation by using a chosen-plaintext attack and one known plaintext ciphertext pair. The minimum execution time of performed attacks indicates the vulnerability of the diffusion-based encryption algorithm. To enhance the security of the understudy cryptographic algorithm, we have also suggested certain improvements.

INDEX TERMS Chaotic map, chosen-plaintext attack, conditional shift, cryptanalysis, Internet of Health Things, known-plaintext attack.

I. INTRODUCTION

With the speedy expansion of computer systems, the most prevalent and unavoidable challenge is providing security to sensitive digital information, although data leakage is common because of the spread of networked computers, storage, and large transmission data. As a result, most of the users on the network are conscious of privacy threats. In multimedia communication, secure transmission and storage of digital data are prime concerns. Cryptography, watermarking, and steganography are used to protect data from illegal and unauthorized access. Among these, cryptography performs a substantial role in extending the privacy of communication over an insecure channel. Cryptography aims to encrypt the data to convert it into unreadable form with the help of a private key. The cryptographic techniques are categorized into block ciphers and stream ciphers. Data is encrypted bit by bit with a secret key generated for encryption in stream ciphers. Linear shift feedback registers (LFSR) are one of the examples of stream cipher and RC4 is the most commonly used stream ciphers. Block cipher involves the encryption of data by converting it into blocks of equal length. The most frequently used block ciphers are Blowfish [1], Data Encryption Standard (DES) [2], Triple Data Encryption Standard (TDES) [3], Advanced Encryption Standard (AES) [4], etc. Since image data requires strong real-time properties, thus these standard encryption structures are appropriate for image encryption. For real-time image encryption, the ciphers demand higher power, processing time, and computational resources. Hence, researchers have offered numerous efficient image encryption techniques [5]–[9] based on various concepts and purposes.

Chaos-based cryptography has been widely utilized for image encryption nowadays [10]–[12]. Chaos is considered a secure source of producing randomness in uniform data. Chaotic systems offer sensitivity to the initial condition, reproduction, ergodicity, non-periodicity, and pseudo-randomness. Moreover, chaotic sequences can be generated accurately and quickly [13]. According to the utilization in

The associate editor coordinating the review of this manuscript and approving it for publication was Chien-Ming Chen.

the image encryption scheme, chaotic maps are partitioned into two groups: one-dimensional chaotic systems and higher dimensional chaotic systems. One-dimensional chaotic maps are easy to implement due to their uncomplicated structure but provide some vulnerabilities due to limited chaotic range. On the other hand, higher-dimensional chaotic maps have better chaotic behavior due to more complicated structures but are hard to implement and have high computational costs. Researchers have offered many secure encryption structures based on higher dimensional chaotic systems.

Chaotic maps offer highly random and secure keys but for a robust cryptosystem, the implementation of secret keys also matters. The robustness of the cryptosystem is assured by the randomness of output data and security against cryptographic attacks. A reliable encryption structure must comprise the phenomenon of diffusion and confusion as offered by Shannon in 1949 [14]. Many proposed encryption schemes ignore the combination of diffusion and confusion which result in a vulnerable encryption structure [15]–[17]. Cryptanalysis is the study of cipher vulnerabilities and methods for exploiting them to determine the plaintext and/or private cipher key. Exploitation is difficult, and several flaws work on the reduced versions of the ciphers. Unfortunately, all the offered cryptosystems claiming the robustness structure are not secure [18]–[21]. There exist many encryption phenomena exhibiting weak security with larger execution time [22]–[27]. The weakness in the encryption structure leads to cryptographic attacks [28]. In this work, we have performed cryptanalysis of a recently proposed encryption technique to secure the Internet of Health Care (IoHT) [30]. The contributions of this work are as follows:

1. We offer an effective strategy for cryptographic attacks that can exploit the diffusion-based cryptosystem with low computation and high security. This is valid particularly in a resource-controlled modern network environment for secure image communication.
2. Our cryptanalysis method is also effective for the other encryption techniques with a similar configuration of diffusion only.
3. By analyzing the security and complexity of the understudy cryptosystem, the corresponding improvements are also suggested, that provide robustness to encryption structure.

The rest of the manuscript is prescribed as subsequent: Section 2 presents some fundamental concepts; The originally offered encryption structure is depicted in section 3; weakness and cryptanalysis are performed in section 4; the next section offers some improvement suggestions and finally conclusion is offered in the last section.

II. SOME BASIC CONCEPTS

A. 2D TRIGONOMETRIC MAP

Robert May proposed a 1D logistic map [23] in 1976 to produce chaotic behavior from a simple nonlinear equation. In mathematical form, the equation of logistic map is defined as:

$$x_{n+1} = r x_n (1 - x_n), \tag{1}$$

where r is bifurcation parameter lies in the interval $[0, 4]$. The sine map in nonlinear dynamics is defined by using sinusoidal function as follows [24]:

$$x_{n+1} = r \sin(\pi x_n), \tag{2}$$

where r is bifurcation parameter lies in the interval $[0, 1]$. Bifurcation diagrams of the logistics map and sine map are depicted in Fig. 1.

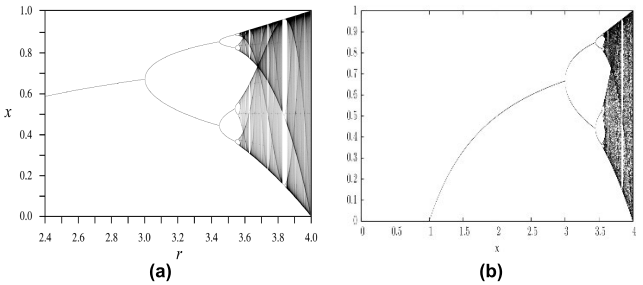

FIGURE 1. Bifurcation diagram of (a) Logistic map (b) Sine map.

A new 2D trigonometric map using logistic and sine maps was offered in [22]. The proposed map can be mathematically elaborated as

$$\begin{cases} x_{n+1} = \sin(\omega x_n) - r \sin(\omega y_n), \\ y_{n+1} = \cos(\omega x_n). \end{cases} \tag{3}$$

The offered map shows chaotic behavior for real numbers of parameters satisfying $\omega = 100\pi, r \in [0, 1000]$, and $x_0 = 1.5, y_0 = 0.5$.

B. HAMMING DISTANCE

Hamming distance between two vectors $\vec{a}, \vec{b} \in \mathbb{F}^n$, can be denoted by $d(\vec{a}, \vec{b})$ and is defined as the number of points where $\vec{a}$ and $\vec{b}$ are different. Therefore, the number of bits required to change one vector into another is known as Hamming distance. Moreover, the bitwise XOR of two vectors $\vec{a}$ and $\vec{b}$ also results in the Hamming distance of bits.

C. MODIFIED MANDELBROT SET

Mandelbrot set is specified as a collection of points in a complex plane. A point Q in the complex plane can be associated with a complex number $q \in C/q = re^{j\theta}$ where θ is the argument of q and r is its magnitude. Mandelbrot set contains a point Q in the complex plane if:

$$\lim_{n\to\infty} \left\| z_{n+1} = z_n^2 + q \right\| \to \infty \quad \text{where } z_0 = 0$$

If a set of points in the complex plane corresponding to the Mandelbrot set are colored in a prism, we attain the shape of Fig. 2.

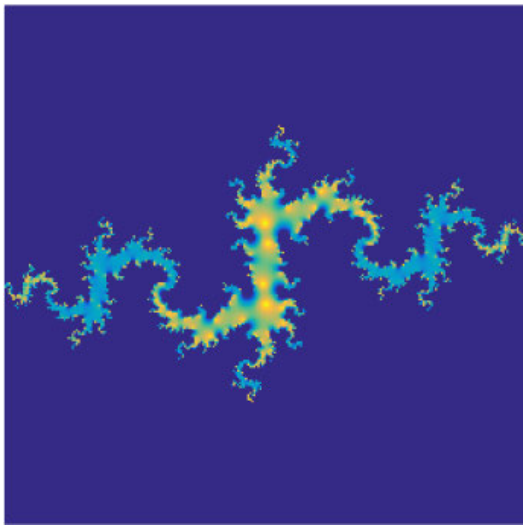

FIGURE 2. The shape of mandelbrot set.

III. EQUIVALENT STRUCTURE OF THE SCHEME OFFERED IN [30]

The understudy technique can be explained in a distinct but corresponding way. Consider that $P^N, N = R, G, B$ and $C^N, N = R, G, B$ be red, green, and blue layers of the plain and encrypted image, respectively. The encryption structure offered in [22] comprises the diffusion of three secret keys based on a 2D trigonometric map, hamming distance, and modified Mandelbrot set.

A. KEY GENERATION

The cryptosystem was based on three private keys. The main attributes for confidentiality were new trigonometric chaotic maps, Mandelbrot set, and hamming distance. The steps leading to key generation are as follows:

Step 1: The first key based on the 2D trigonometric map was determined by finding the solution trajectories of system (1) with some specific initial conditions and bifurcation parameters. The generated chaotic sequences are named as $\zeta^i,\ 1 \le i \le 3$. The key set K_1 concerning image channels can be characterized as:

$$K_1 = \left\{\zeta^i, 1 \le i \le 3\right\}. \tag{4}$$

Step 2: The second key established on the hamming distance was attained by original image components and chaotic sequences. The mathematical strides pursued in the generation of the second encryption key can be specified as follows:

$$\Delta^i = d\left(P^N, \zeta^i\right), \tag{5}$$

where d denoted the hamming distance among plain image channels and chaotic sequences, ζ^i is the chaotic sequences for $1 \le i \le 3$, and $P^N, N = R, G, B$ represents red, green, and the blue channel of the plain image. The second private key set K_2 according to layers of the image can be defined as:

$$K_2 = \left\{\Delta^i, 1 \le i \le 3\right\}. \tag{6}$$

Step 3: The third encryption key was acquired by using the conditional shift algorithm on the trajectories obtained from the Mandelbrot set $\psi^i, 1 \le i \le 3$ and diffusion of original image layers with the key set K_1 as:

$$\lambda^i = P^N \oplus \zeta^i. \tag{7}$$

The conditional shift was applied on $\psi^i, 1 \le i \le 3$ and $\lambda^i, 1 \le i \le 3$ by using the algorithm defined in Table 1.

TABLE 1. Algorithm for the conditional shift.

Input: Sequences from Mandelbrot set $\psi^i, 1 \le i \le 3$ and output of XOR between chaotic sequences and image layer that is $\lambda^i, 1 \le i \le 3$.

Output: $\alpha^i, 1 \le i \le 3$ are the final shifted matrices for $\lambda^i, 1 \le i \le 3$ respectively.

while j=0 to n do

// n shows the number of columns in ψ^1, ψ^2, ψ^3

$\max_j$ *(jth rows of* (ψ^1, ψ^2, ψ^3)*)*

apply shift as follows:

phase 1 *do if* $\left(\max_j \le \max_{j1}\right)$ *then*

apply $\max_j$ *time left cyclic shift on the* j^{th} *row of* ψ^1

else apply $\max_j$ *time right cyclic shift on the* j^{th} *row of* ψ^1

end

phase 2 *do if* $\left(\max_j \le \max_{j2}\right)$ *then*

apply $\max_j$ *time left cyclic shift on the* j^{th} *row of* ψ^2

else apply $\max_j$ *time right cyclic shift on the* j^{th} *row of* ψ^2

end

phase 3 *do if* $\left(\max_j \le \max_{j3}\right)$ *then*

apply $\max_j$ *time left cyclic shift on the* j^{th} *row of* ψ^3

else apply $\max_j$ *time right cyclic shift on the* j^{th} *row of* ψ^3

end

The final encryption key obtained after the conditional shift is represented by the set K_3.

$$K_3 = \left\{\alpha^i, 1 \le i \le 3\right\}. \tag{8}$$

B. ENCRYPTION SCHEME

The encryption scheme offered by authors in [22] can be depicted by the subsequent steps:

Step 1: Insert color original image P^N and separate it into the red, green, and blue layers equally $N = R, G, B$ correspondingly as input of the encryption algorithm.

Step 2: The cipher obtained in step 2 is diffused with the key obtained from the Hamming distance in the

following ways:

$$\lambda^i = P^N \oplus \zeta^i, \tag{9}$$

where $N = R, G, B$ and $1 \leq i \leq 3$ respectively for each channel of the color image.

Step 3: The diffusion of ciphers obtained in step 2 along with the second hamming distance based secret key by the following procedure:

$$\eta^i = \lambda^i \oplus \Delta^i, \tag{10}$$

Step 4: Last encryption key based on conditional is diffused with the ciphers obtained from the previous step by:

$$C^N = \eta^i \oplus \alpha^i, \tag{11}$$

The obtained resultant $C^N, N = R, G, B$, are red, green, blue layers of the cipher image, respectively.

The encryption structure can be summarized into the equivalent system as

$$C^N = P^N \oplus \zeta^i \oplus \Delta^i \oplus \alpha^i, \tag{12}$$

where ζ^i represents the key from chaotic sequences, Δ^i is the key generated from a hamming distance, α^i shows the key constructed by conditional shift algorithm, and $1 \leq i \leq 3$ for the red, green, and blue channel of the original and enciphered images respectively.

C. EQUIVALENT ENCRYPTION STRUCTURE

The encryption structure defined in Eq. (12) can be converted into a simpler form by looking at the detailed implementation phenomenon of the keys. The first key is utilized by the bitwise addition operation with the plaintext as:

$$\lambda^i = P^N \oplus \zeta^i, \tag{13}$$

Now we come to the second key implementation as:

$$\eta^i = \lambda^i \oplus \Delta^i, \tag{14}$$

By using (13) in (14) we get

$$\eta^i = P^N \oplus \zeta^i \oplus \Delta^i, \tag{15}$$

where $\Delta^i = d\left(P^N, \zeta^i\right)$ is the hamming distance between original image layers and chaotic sequences. Now we check the working of hamming distance operation for two binary numbers to get a generalized result, for example:

$$d\,(01001001, 10100111) = 11101110$$

Also

$$01001001 \oplus 10100111 = 11101110$$

This result is satisfied by all the binary numbers. This indicates that hamming distance works as a bitwise addition operation. Therefore, the hamming distance of the original image and chaotic sequence is the bitwise addition of each element one by one. Hence after generalizing this result, we can write:

$$\Delta^i = d\left(P^N, \zeta^i\right) = P^N \oplus \zeta^i, \tag{16}$$

Using (16) in (15) we get@comm

$$\eta^i = P^N \oplus \zeta^i \oplus P^N \oplus \zeta^i = 0, \tag{17}$$

This reflects that both λ^i and η^i cancel the effect of each other because both possess the same elements. Therefore, using the result of (17) in (11) we get.

$$C^N = 0 \oplus \alpha^i = \alpha^i, \tag{18}$$

where $\alpha^i, 1 \leq i \leq 3$ is the key obtained from the conditional shift. The ciphertext can be defined as:

$$C^N = \alpha^i(P^N). \tag{19}$$

The understudy cryptosystem produces ciphers with the operation of conditional shift by using Mandelbrot sequences. The conditional shift algorithm permutes the data concerning the plaintext.

The structural diagram of the equivalent cryptosystem is displayed in Fig. 3.

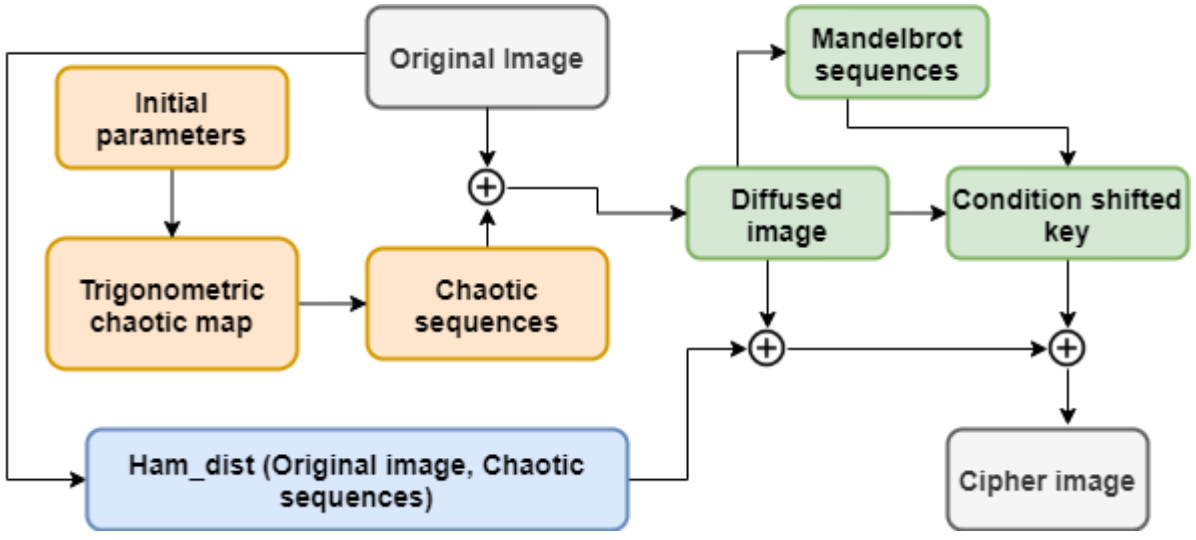

FIGURE 3. Equivalent illustration of understudy cryptosystem.

IV. WEAKNESSES AND CRYPTANALYSIS OF UNDERSTUDY CRYPTOSYSTEM [30]

A. WEAKNESS IN UNDERSTUDY CRYPTOSYSTEM

The cryptosystem based on the diffusion strategy offered in [30] aimed to provide security to data on the Internet of Healthcare Things (IoHT). The contribution of the suggested algorithm was the deployment of three secret keys to specify security in encryption. The drawback of the offered scheme was the process of diffusion only. The originally proposed scheme possesses the implementation of chaos, hamming distance, and conditional shift. But the operation of bitwise XOR and hamming distance reflects the same behavior, which terminates the effect of each other after diffusion as depicted in (16) and (17). According to Shannon's theory provided in 1949 [14], a secure cryptosystem must fabricate confusion and diffusion in cipher data. The understudy cryptosystem neglects the phenomenon of confusion and yields diffusion only with a complex encryption phenomenon and larger execution time. The outcomes in the simplified version of the encryption scheme just perform permutation using a conditional shift algorithm. Therefore, diffusion which reduces to permutation only in simpler version can be effortlessly broken by applying conventional assaults such as known-plaintext attack and chosen-plaintext attack. The offered attack aims to retrieve the plaintext from its respective ciphertext without knowing the security parameters of the cryptosystem. The offered attacks are performed in the following way:

B. KNOWN-PLAINTEXT ATTACK

Suppose that the assailant gets a pair of plaintext and ciphertext encrypted through the understudy cryptosystem. The description of the final cryptosystem is defined in (12). From the equivalent cryptosystem, we can notice that the encryption design was based on the diffusion of three private keys with plaintext, but diffusion and hamming distance dismiss each other effect and it reduces to (13). Understudy equivalent cryptosystem can also be generalized for the greyscale image. The working strides of known-plaintext attack are delineated as follows:

Suppose we are aware of one pair of plaintext and ciphertext having size $m \times n$ produced from the originally proposed encryption structure, that is

$$P = \begin{bmatrix} P_{11} & P_{12} & \cdots & P_{1n} \\ P_{21} & P_{22} & \cdots & P_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ P_{m1} & P_{m2} & \cdots & P_{mn} \end{bmatrix},$$

$$C = \begin{bmatrix} C_{11} & C_{12} & \cdots & C_{1n} \\ C_{21} & C_{22} & \cdots & C_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ C_{m1} & C_{m2} & \cdots & C_{mn} \end{bmatrix}_{m\times n},$$

As we know that the ciphertext is generated by using the conditional shift algorithm as defined in (19)

$$C = \alpha\left(P\right),$$

After checking the one-to-one correspondence between the elements of plain and cipher matrix the original sorting position of particles can be retrieved.

C. CHOSEN-PLAINTEXT ATTACK

The chosen-plaintext attack works on the phenomenon of insertion of the desired plaintext in the cryptosystem. Further, the plaintexts and respectively produced ciphers are assessed to retrieve the key. Suppose the assailant gets short-term entrance to the encryption mechanism. Hence, the assailant selected a plain image with all possible entries increasing one by one as input of the encryption algorithm.

$$P = \begin{bmatrix} 0 & 1 & \cdots & n \\ n+1 & n+2 & \cdots & 2n \\ \vdots & \vdots & \ddots & \vdots \\ (m-1)n+1 & (m-1)n+2 & \cdots & mn \end{bmatrix}_{m\times n},$$

where $m \times n$ is the size of the image to be retrieved. The equivalent description of the cryptosystem is defined in Eq. (12). From the equivalent cryptosystem, we can notice that the encryption design was based on the permutation using conditional shift key as depicted in Eq. (19). Understudy equivalent cryptosystem can also be generalized for the greyscale image. The working strides of known-plaintext attack are delineated as follows:

Consider

$$C = \begin{bmatrix} C_{11} & C_{12} & \cdots & C_{1n} \\ C_{21} & C_{22} & \cdots & C_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ C_{m1} & C_{m2} & \cdots & C_{mn} \end{bmatrix}_{m\times n},$$

After inserting these values in Eq. (15) we ge

$$C = \alpha(P) = \alpha\left(\begin{bmatrix} 0 & 1 & \cdots & n \\ n+1 & n+2 & \cdots & 2n \\ \vdots & \vdots & \ddots & \vdots \\ (m-1)n+1 & (m-1)n+2 & \cdots & mn \end{bmatrix}\right)$$

$$\alpha(P) = \begin{bmatrix} C_{11} & C_{12} & \cdots & C_{1n} \\ C_{21} & C_{22} & \cdots & C_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ C_{m1} & C_{m2} & \cdots & C_{mn} \end{bmatrix}_{m\times n}$$

where α is the conditional shift key. Therefore, we get the position of each pixel in the resultant cipher. After the comparison of both chosen-plaintext and respective cipher data, the shift of each element can be obtained. There exists a one-to-one correspondence of each plaintext element with its respective ciphertext due to elementwise addition operation.

The correspondence between elements is defined by:

$$C_{ij} = \alpha\left(P_{ij}\right),$$

Hence the plaintext is retrieved by using the correspondence between elements.

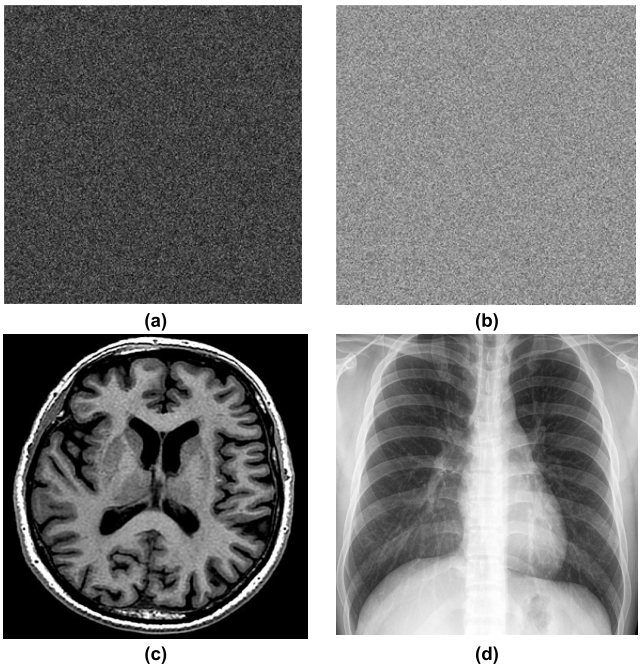

FIGURE 4. (a), (b) Cipher images encrypted by understudy scheme; (c), (d) Recovered original images by the chosen-plaintext attack.

The chosen image and recovered image are depicted in Fig. 4.

D. EXPERIMENTAL RESULTS

The working strides of the chosen-plaintext attack are described in this section with a numerical example. The plaintext is retrieved by two steps; the first is the detection of elements of ciphertext C_{ij} and the second one is finding the position of the element in their respective plaintext. Hence, the plaintext of each ciphertext is extracted without knowing a specific key because the secret key is changed for the input.

We have considered a small example with a plaintext and ciphertext domain as $\mathbb{Z}_4$, or in other words algorithm is explored over 2-bits and data set in the form of 3×3 matrix. Therefore, the elements of plain and cipher data belong from the set $\mathbb{Z}_4 = \{0, 1, 2, 3\}$, same is the case with the secret key.

The results in Table 2 depicts the different chosen-plaintext matrix and their respective ciphers. The outcomes of the table also support the argument in (16) and (17) that is the whole encryption process depends on the conditional shift key only because diffusion and hamming distance abandon each other effect. These four pairs of plaintexts and ciphertext help to retrieve the original image encrypted by the understudy cipher scheme in the following way:

Suppose C be the ciphertext matrix encrypted by the understudy scheme.

$$C = \begin{bmatrix} 2 & 3 & 1 \\ 1 & 2 & 0 \\ 1 & 0 & 3 \end{bmatrix},$$

As we can see that

$$C_{11} = 2$$

From the ciphers C^1, C^2, C^3, C^4 the C^2 has $C^2_{11} = 2$ and its respective original element is in P_3 that is $P^3_{11} = 2$. Similarly, for $C_{12} = 3$ the cipher $C^4_{12} = 3$ and its respective original element is in P_4 that is $P^4_{12} = 3$.

For $C_{13} = 1$ the cipher $C^1_{13} = 1$ and its respective original element is in P_1 that is $P^1_{13} = 0$.

For $C_{21} = 1$ the cipher $C^2_{21} = 1$ and its respective original element is in P_2 that is $P^2_{21} = 1$.

TABLE 2. Results of chosen-plaintext attack.

Chosen-plaintext	Secret keys generated by the cryptosystem and unknown to attacks			Respective ciphertext
	Independent key	Plaintext dependent key		
	Chaotic key	Ham distance key	Conditional shift key	
$P^1 = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$	$\begin{bmatrix} 1 & 0 & 3 \\ 3 & 2 & 1 \\ 2 & 0 & 3 \end{bmatrix}$	$\begin{bmatrix} 1 & 0 & 3 \\ 3 & 2 & 1 \\ 2 & 0 & 3 \end{bmatrix}$	$\begin{bmatrix} 0 & 2 & 1 \\ 0 & 1 & 3 \\ 3 & 2 & 2 \end{bmatrix}$	$C^1 = \begin{bmatrix} 0 & 2 & 1 \\ 0 & 1 & 3 \\ 3 & 2 & 2 \end{bmatrix}$
$P^2 = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix}$	$\begin{bmatrix} 1 & 0 & 3 \\ 3 & 2 & 1 \\ 2 & 0 & 3 \end{bmatrix}$	$\begin{bmatrix} 0 & 1 & 2 \\ 2 & 3 & 0 \\ 3 & 1 & 2 \end{bmatrix}$	$\begin{bmatrix} 2 & 1 & 3 \\ 1 & 2 & 0 \\ 2 & 3 & 1 \end{bmatrix}$	$C^2 = \begin{bmatrix} 2 & 1 & 3 \\ 1 & 2 & 0 \\ 2 & 3 & 1 \end{bmatrix}$
$P^3 = \begin{bmatrix} 2 & 2 & 2 \\ 2 & 2 & 2 \\ 2 & 2 & 2 \end{bmatrix}$	$\begin{bmatrix} 1 & 0 & 3 \\ 3 & 2 & 1 \\ 2 & 0 & 3 \end{bmatrix}$	$\begin{bmatrix} 3 & 2 & 1 \\ 1 & 0 & 3 \\ 0 & 1 & 2 \end{bmatrix}$	$\begin{bmatrix} 3 & 0 & 2 \\ 2 & 3 & 1 \\ 0 & 1 & 0 \end{bmatrix}$	$C^3 = \begin{bmatrix} 3 & 0 & 2 \\ 2 & 3 & 1 \\ 0 & 1 & 0 \end{bmatrix}$
$P^4 = \begin{bmatrix} 3 & 3 & 3 \\ 3 & 3 & 3 \\ 3 & 3 & 3 \end{bmatrix}$	$\begin{bmatrix} 1 & 0 & 3 \\ 3 & 2 & 1 \\ 2 & 0 & 3 \end{bmatrix}$	$\begin{bmatrix} 2 & 3 & 0 \\ 0 & 1 & 2 \\ 1 & 3 & 0 \end{bmatrix}$	$\begin{bmatrix} 1 & 3 & 0 \\ 2 & 0 & 2 \\ 1 & 0 & 3 \end{bmatrix}$	$C^4 = \begin{bmatrix} 1 & 3 & 0 \\ 2 & 0 & 2 \\ 1 & 0 & 3 \end{bmatrix}$

For $C_{22} = 2$ the cipher $C_{22}^2 = 1$ and its respective original element is in P_2 that is $P_{21}^2 = 1$.

Similarly, checking the correspondence of all other elements of ciphertext with its respective chosen-plaintext the recovered plaintext matrix becomes,

$$P = \begin{bmatrix} 2 & 3 & 0 \\ 1 & 1 & 1 \\ 3 & 3 & 3 \end{bmatrix}$$

which is the retrieved plaintext without getting the key. Therefore, we can also recover any plaintext from the respective cipher value even if its secret key is changed concerning the plaintext.

E. EXECUTION TIME ANALYSIS

The execution time of attacks performed to retrieve the image of different sizes reveals the vulnerability in the encryption phenomenon. All the attacks were performed on a personal computer with an Intel(R) for the simulations. Core (TM) i7-7500U 2.90 GHz CPU and 12 GB memory capacity. MATLAB R2018b was utilized for the simulations. The execution time of the chosen-plaintext attack and known-plaintext attack in seconds for various sizes of images are presented in Table 3.

TABLE 3. Execution time (seconds) analysis.

Image size	Chosen-plaintext attack	Known-plaintext attack
128×128	0.56	0.42
256×256	1.20	0.97
512×512	1.73	1.32
1024×1024	2.01	1.81

The results in Table 2 reflect that image with the size 1024×1024 can be retrieved in less than 2 seconds by using the known-plaintext attack. The less execution time reveals weakness of the cryptosystem due to which it was breakable with low computation.

V. IMPROVEMENT SUGGESTIONS

The security of the originally proposed scheme can be increased by introducing the concept of confusion and diffusion according to Shannon's theory [14]. The originally offered encryption scheme uses the concept of diffusion only and ignores the confusion phenomenon. Some suggestions to improve the security of encryption structure are as follows:

1. The confusion can be generated by using some Substitution box constructed from a chaotic system.
2. The key form Mandelbrot set may produce diffusion in encryption structure by using the XOR operation.
3. The conditional shift algorithm must be applied directly to the original image instead of employing the key to the XOR operation.

The above-stated improvement suggestions can be implemented to intensify the security of the encryption structure. The chosen-plaintext attack and known-plaintext attack are futile in breaking the combination confusion and diffusion strategy. Therefore, the suggested improvements resist all possible classical and statistical cryptographic attacks.

VI. CONCLUSION

In this work, we have reported some classical attacks on a recently proposed encryption technique. The originally proposed encryption structure comprises a chaotic system, modified Mandelbrot set, and conditional shift algorithm that possess some weaknesses in its designed structure. In information security, proposing a scheme based on individual XOR operations for encryption is considered a weak strategy. The offered attacks are performed with very little computation by using chosen plain image and known-plaintext and ciphertext pair. Consequently, the understudy encryption technique is vulnerable to compete with the Internet of Health Things (IoHT) security. The encryption scheme offered by authors in [22] is not recommended for secure encryption in its present form. Therefore, we have offered some improvement suggestions to intensify the security of IoHT. The cryptosystem constructed with the stated improvement suggestion can be utilized for secure communication.

REFERENCES

[1] B. Schneier, "Fast software encryption," in *Proc. Cambridge Secur. Workshop*. U.K.: Springer-Verlag, 1994, pp. 191–204.
[2] A. Biryukov and C. De Canniére, "Data encryption standard (DES)," in *Encyclopedia of Cryptography and Security*, H. C. Van Tilborg, Ed. Boston, MA, USA: Springer, 2005, doi: 10.1007/0-387-23483-7_94.
[3] C. De Cannière, "Triple-DES," in *Encyclopedia of Cryptography and Security*, H. C. Van Tilborg, Ed. Boston, MA, USA: Springer, 2005, doi: 10.1007/0-387-23483-7_437.
[4] M. Dworkin, E. Barker, J. Nechvatal, J. Foti, L. Bassham, E. Roback, and J. Dray, "Advanced encryption standard (AES)," Federal Inf. Process. Stds., Nat. Inst. Standards Technol., Gaithersburg, MD, USA, Tech. Rep., 2005, doi: 10.6028/NIST.FIPS.197.
[5] G. Cheng, C. Wang, and H. Chen, "A novel color image encryption algorithm based on hyperchaotic system and permutation-diffusion architecture," *Int. J. Bifurcation Chaos*, vol. 29, no. 9, Aug. 2019, Art. no. 1950115.
[6] L. Gong, K. Qiu, C. Deng, and N. Zhou, "An image compression and encryption algorithm based on chaotic system and compressive sensing," *Opt. Laser Technol.*, vol. 115, pp. 257–267, Jul. 2019.
[7] M. Khan, F. Masood, A. Alghafis, M. Amin, and S. I. B. Naqvi, "A novel image encryption technique using hybrid method of discrete dynamical chaotic maps and brownian motion," *PLoS ONE*, vol. 14, no. 12, Dec. 2019, Art. no. e0225031, doi: 10.1371/journal.pone.0225031.
[8] Z.-J. Huang, S. Cheng, L.-H. Gong, and N.-R. Zhou, "Nonlinear optical multi-image encryption scheme with two-dimensional linear canonical transform," *Opt. Lasers Eng.*, vol. 124, Jan. 2020, Art. no. 105821.
[9] F. Masood, W. Boulila, J. Ahmad, Arshad, S. Sankar, S. Rubaiee, and W. J. Buchanan, "A novel privacy approach of digital aerial images based on mersenne twister method with DNA genetic encoding and chaos," *Remote Sens.*, vol. 12, no. 11, p. 1893, Jun. 2020.
[10] N. Zhou, X. Yan, H. Liang, X. Tao, and G. Li, "Multi-image encryption scheme based on quantum 3D Arnold transform and scaled Zhongtang chaotic system," *Quantum Inf. Process.*, vol. 17, no. 12, p. 36, Dec. 2018.
[11] A. Alghafis, N. Munir, M. Khan, and I. Hussain, "An encryption scheme based on discrete quantum map and continuous chaotic system," *Int. J. Theor. Phys.*, vol. 59, no. 4, pp. 1227–1240, Apr. 2020, doi: 10.1007/s10773-020-04402-7.
[12] F. Masood, J. Ahmad, S. A. Shah, S. S. Jamal, and I. Hussain, "A novel hybrid secure image encryption based on julia set of fractals and 3D Lorenz chaotic map," *Entropy*, vol. 22, no. 3, p. 274, 2020.
[13] N. Munir, M. Khan, Z. Wei, A. Akgul, M. Amin, and I. Hussain, "Circuit implementation of 3D chaotic self-exciting single-disk homopolar dynamo and its application in digital image confidentiality," *Wireless Netw.*, vol. 4, pp. 1–8, May 2020, doi: 10.1007/s11276-020-02361-9.

[14] C. E. Shannon, "Communication theory of secrecy systems," *Bell Labs Tech. J.*, vol. 28, no. 4, pp. 656–715, Oct. 1949.
[15] S. Dhall, S. K. Pal, and K. Sharma, "Cryptanalysis of image encryption based on a new 1D chaotic system," *Signal Process.*, vol. 1684, no. 17, pp. 30434–30436, 2017, doi: 10.1016/j.sigpro.2017.12.021.
[16] Y. Liu, L. Y. Zhang, J. Wang, Y. Zhang, and K.-W. Wong, "Chosen-plaintext attack of an image encryption scheme based on modified permutation–diffusion structure," *Nonlinear Dyn.*, vol. 84, no. 4, pp. 2241–2250, Jun. 2016.
[17] Y. Zhang, D. Xiao, W. Wen, and H. Nan, "Cryptanalysis of image scrambling based on chaotic sequences and Vigenère cipher," *Nonlinear Dyn.*, vol. 78, no. 1, pp. 235–240, Oct. 2014.
[18] N. Munir, M. Khan, T. Shah, A. S. Alanazi, and I. Hussain, "Cryptanalysis of nonlinear confusion component based encryption algorithm," *Integration*, vol. 79, pp. 41–47, Jul. 2021, doi: 10.1016/j.vlsi.2021.03.004.
[19] R. Rhouma and S. Belghith, "Cryptanalysis of a chaos-based cryptosystem on DSP," *Commun. Nonlinear Sci. Numer. Simul.*, vol. 16, no. 2, pp. 876–884, Feb. 2011.
[20] F.-G. Jeng, W.-L. Huang, and T.-H. Chen, "Cryptanalysis and improvement of two hyper-chaos-based image encryption schemes," *Signal Process., Image Commun.*, vol. 34, pp. 45–51, May 2015.
[21] E. Solak, R. Rhouma, and S. Belghith, "Breaking an orbit-based symmetric cryptosystem," *Math. Comput. Model.*, vol. 54, nos. 5–6, pp. 1413–1419, Sep. 2011.
[22] N. Tsafack, S. Sankar, B. Abd-El-Atty, J. Kengne, J. K. C., A. Belazi, I. Mehmood, A. K. Bashir, O.-Y. Song, and A. A. A. El-Latif, "A new chaotic map with dynamic analysis and encryption application in Internet of Health Things," *IEEE Access*, vol. 8, pp. 137731–137744, 2020, doi: 10.1109/ACCESS.2020.3010794.
[23] G.-C. Wu and D. Baleanu, "Chaos synchronization of the discrete fractional logistic map," *Signal Process.*, vol. 102, pp. 96–99, Sep. 2014.
[24] Z. Hua, B. Zhou, and Y. Zhou, "Sine chaotification model for enhancing chaos and its hardware implementation," *IEEE Trans. Ind. Electron.*, vol. 66, no. 2, pp. 1273–1284, Feb. 2019.
[25] A. Churcher, R. Ullah, J. Ahmad, S. ur Rehman, F. Masood, M. Gogate, F. Alqahtani, B. Nour, and W. J. Buchanan, "An experimental analysis of attack classification using machine learning in IoT networks," *Sensors*, vol. 21, no. 2, p. 446, Jan. 2021.
[26] A. Qayyum, J. Ahmad, W. Boulila, S. Rubaiee, Arshad, F. Masood, F. Khan, and W. J. Buchanan, "Chaos-based confusion and diffusion of image pixels using dynamic substitution," *IEEE Access*, vol. 8, pp. 140876–140895, 2020.
[27] I. E. Hanouti, H. E. Fadili, W. Souhail, and F. Masood, "A lightweight pseudo-random number generator based on a robust chaotic map," in *Proc. 4th Int. Conf. Intell. Comput. Data Sci. (ICDS)*, Oct. 2020, pp. 1–6.
[28] N. Munir, M. Khan, S. S. Jamal, M. M. Hazzazi, and I. Hussain, "Cryptanalysis of hybrid secure image encryption based on Julia set fractals and three-dimensional Lorenz chaotic map," *Math. Comput. Simul.*, vol. 190, pp. 826–836, Dec. 2021, doi: 10.1016/j.matcom.2021.06.008.

NOOR MUNIR is currently pursuing the Ph.D. degree with the Department of Applied Mathematics and Statistics, Institute of Space Technology. Her area of specialization is cryptanalysis. She is currently working with cryptanalysis of various chaos encryption algorithms.

MAJID KHAN received the Ph.D. degree in mathematics from Quaid-i-Azam University Islamabad, Pakistan, in December 2015. He is currently working as an Assistant Professor with the Department of Applied Mathematics and Statistics, Institute of Space Technology, Islamabad, Pakistan. His research interests include chaotic cryptography, algebraic cryptography, digital information hiding, and multi-criteria decision making.

MOHAMMAD MAZYAD HAZZAZI received the Ph.D. degree in mathematics from the University of Sussex, Brighton, U.K. He is currently working as an Assistant Professor with the Department of Mathematics, King Khalid University, Abha, Saudi Arabia. His research interests include coding theory, cryptography, finite geometry, algebraic geometry, and group theory.

AMER ALJAEDI received the B.Sc. degree from King Saud University, Saudi Arabia, in 2007, the M.Sc. degree in information systems security from the Concordia University of Edmonton, Canada, in 2011, and the Ph.D. degree in security engineering from the Computer Science Department, Colorado University, Colorado Springs, USA, in 2018. He is currently an Assistant Professor with the College of Computing and Information Technology, University of Tabuk. Before that, he was a Senior Research Member with the Cybersecurity Laboratory, Colorado University, and he received multiple research awards from UCCS and SACM for his outstanding research articles. His research interests include software-defined networking, network traffic control and monitoring, cloud computing, and cybersecurity.

ABD AL KARIM HAJ ISMAIL is currently an Active Researcher in the field of high energy physics and data analysis. He started his scientific career in the detection of cosmic radiations and measure their energy spectrum. He currently expanded his research interest to be involved in a couple of research projects, such as cosmic rays, dark matter, solar radiation analysis, and data analysis.

ADEL R. ALHARBI received the B.Sc. degree in computer science from Qassim University, Saudi Arabia, in 2008, and two M.Sc. degrees in security engineering and computer engineering and the Ph.D. degree in Computer Engineering from Southern Methodist University, Dallas, TX, USA, in 2013, 2015, and 2017, respectively. He has been a Faculty Staff Member with the College of Computing and Information Technology, University of Tabuk, Saudi Arabia, since 2009. He acquired several academic certificates and published many scientific articles. His research interests include mobile and smart device applications, biometric, security, networking, and machine learning techniques.

IQTADAR HUSSAIN received the Ph.D. degree in mathematics from Quaid-i-Azam University, Pakistan, in 2014. He has developed many new construction mechanisms for nonlinear confusion component of block ciphers. He is currently an Assistant Professor with Qatar University. He added new structures in cryptology and its applications in various digital contents privacy. His research interests include applications of mathematical concepts in secure communication and cybersecurity.