Received: January 16, 2022. Revised: February 18, 2022.

International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

Image Cryptosystem for IoT Devices Using 2-D Zaslavsky Chaotic Map

Ahmed H. Mohammed[1]* **Ahmed Kareem Shibeeb[2]** **Mohammed Hussein Ahmed[1]**

[1]*Department of Computer Science, College of Education, Mustansiriyah University, Baghdad, Iraq*
[2]*Department of Computer Systems, Technical Institute – Suwaira, Middle Technical University, Baghdad, Iraq*
* Corresponding author's Email: dr.ahmedh@uomustansiriyah.edu.iq

Abstract: Recently, the proliferation of the Internet of Things (IoT) services and applications has prompted several governments to deploy many cameras in critical sites, such as embassies, military institutions, and ministries. The images must be encrypted to protect data shared between IoT sensors/devices and embedded subsystems. Often, IoT devices are smaller and less powerful. A lot of traditional encryption methods are computationally inefficient. They require many rounds of coding, which takes up much space on a device. Despite this, this paper has developed a lightweight encryption algorithm based on chaos theory suitable for IoT devices with limited processing power. The confusion-diffusion structure is often divided into two independent components in chaotic image cryptosystems. However, it reduces the security of the cryptosystem since the independent design may be subjected to cryptanalysis individually. This paper presents an efficient chaotic image encryption algorithm based on a plaintext-associated approach. It incorporates confusion-diffusion operation to increase encryption reliability. The Zaslavsky map initial values are determined by the values and locations of an input image and random values to resist chosen-plaintext cryptanalysis. Furthermore, the proposed method uses a simultaneous confusion-diffusion process to resist any separate attack. The simulation and experimental analysis demonstrate that the proposed encryption algorithm has 0.3927 seconds as a fast encryption time. Moreover, it provides a high performance compared to several other chaotic-based image cryptosystems. as measured by the histogram, entropy (7.99723), pixel change rate (99.7194), unified average changing intensity (33.4635) within the critical interval, pixel correlation, global and local entropy, CDR (ciphertext difference rate), and gray difference degree (GDD). It also has higher security than other chaotic-based image cryptosystems.

Keywords: IoT, Zaslavsky map, Simultaneous confusion-diffusion, Image encryption.

1. Introduction

The internet is one of the essential technologies for enhancing all aspects of life. It is a more extensive network of things with various sensors, actuators, and microcontrollers that enables "things" to send and receive data in the form of images, music, video, signals, text, and other types of data from all over the world [1]. The IoT is predicted to connect billions of users with billions of networked devices interacting in real-time [2]. The IoT is the new tech of our age, with billions of electronic gadgets sharing massive amounts of protected data. The private image collected by industrial IoT has evolved and is linked to the user's IoT nodes or peripheral devices [3]. Multimedia has developed rapidly with the introduction of internet technologies, allowing people to share data in images, video, audio, biometric images, medical imaging, military, diplomatic, national security agencies, and their equivalents in the IoT [4, 5]. Image data security, including sensitive healthcare and military applications, has become increasingly important because it led to various transmission violations of sensitive images and is vulnerable to interception while being sent across the internet [6]. The flexible and secure solution to ensuring the confidentiality of images in IoT systems is the encryption method [7]. There are two issues concerning IoT-based image encryption. The first issue with IoT applications is protecting the enormous amounts of data provided by heterogeneous IoT devices, which might be targeted for cyber-attacks [8]. The second issue is that IoT comes with many restricted devices connected over the network to interact with users and IoT services [9]. Cryptography is a specific branch of communication security science that conceals the content of data transmissions also used in IoT applications based on two types. Firstly, symmetric algorithms use the identical key safely sent between the sender and the recipient for encryption and decryption [10]. Secondly, Asymmetric algorithms use two distinct keys, the public key transmitted between parties and private keys that are never broadcast across the network to ensure security. Even if the hacker had the public key, he could not decipher the encrypted message unless the secret key was known to him [11]. Asymmetric algorithms required more resources and were more challenging to implement than symmetric algorithms. Most IoT applications use symmetric algorithms because they are simple to construct, consume fewer resources, and more secure as long as adversaries find it challenging to crack the key [12]. Lightweight cryptography refers to cryptographic methods that ensure low memory demands and execution time with limited resources to meet the needs of IoT applications. At the same time, lightweight methods must satisfy the application's security requirements [13]. Standard encryption methods, such as MD5, IDEA, AES, and others, are not proper for encryption in IoT because of sensor and device resources limits. Moreover, image features are highly relative between neighboring pixels, and data redundancy necessitates complex specific processing capabilities [14].

In chaotic image cryptosystems, the confusion-diffusion structure is usually split into two halves which yields a weaker cryptosystem since each different design may be cryptanalysis. This paper is improved by using the confusion-diffusion procedure and plaintext-associated technique to provide an efficient chaotic image encryption algorithm. Following iteration of the Zaslavsky map, we arrange ting matrices in ascending and descending order for permutation and diffusion operations, respectively. At the end of the process, the combined permutation-diffusion approach is employed to confuse and disperse image information simultaneously.

2. Related work

There are a variety of approaches that can be used to protect data from IoT devices. On the other hand, image encryption continues to have some limitations in terms of how quickly it can be completed and how secure it is. This paper aims to develop a reliable image encryption method for IoT devices, emphasising the numerous chaotic image cryptosystems recently introduced for IoT applications.

Seema et al. (2019) proposed an image encryption-based chaotic logistic map with confusion and diffusion process where the logistic parameter is taken as the encryption key and attuned to adopting the LCA algorithm [15]. Lixiang et al. (2020) suggested a compressed sensing (CS) model based on chaotic systems for sending images securely and satisfying IoT further of resource-constrained by adopting a corresponding parallel reconstruction algorithm in IoT application [16]. Andrew Boutros et al. (2017) combined two types of chaotic maps, the Arnold's Cat and the cascaded discrete duffing equations for image cryptosystem with confusion and diffusion [17]. Ahmad et al. (2019) coupled two chaotic (lightweight Chebyshev and Intertwining) maps for image encryption with Lifting Wavelet Transform (LWT), further enhancing confusion and diffusion processes [18]. Omrani and Sliman (2019) proposed a cryptography system based on Extended CatMap to maintain a low correlation of the data content and reduce the critical factor processing time and memory use in IoT [19]. K. Rarhi and S. Saha (2020) merged two hyperchaotic maps for image encryption, the Lorenz attractor with the Rossler system; besides, they employed the DNA encoding techniques and neural network to manage the permutation and substitution image encryption process [20]. E.E. Garcíahi (2020) improved the randomness of five chaotic maps to encrypt images across wireless communication schemes and implemented them in PIC-microcontroller via ZigBee channels [21]. Y. Zhang et al. (2020) proposed an image encryption-based neural network and XoR operation with the key generated by chaotic systems and the S-box of AES to achieve diffusion [22]. Z. Hua and colleagues (2020) developed an encryption algorithm for images with three color planes based on a two-dimensional logistic tent modular map (2DLTMM) [23]. Guangfeng C et al. (2020) have proposed a color-image encryption technique that uses hyperchaotic and permute-diffusion through combining R, G, and B components and increasing the dependence of each variable on the others [24]. Manish G et al. (2021) proposed symmetric image encryption based on the double point crossover and uniform mutation operators [25]. Land et al. (2020) suggested using message transmission and a two-logistic map to produce pseudorandom edge pixel sets [26]. Siva J et al. (2020) implemented an image encryption method with chaotic system qualities was constructed on a 32-bit microcontroller with chaos system traits to encrypt grayscale images [27]. S. Satyabrata et al. (2021). suggested an efficient, lightweight, and secure image encryption method based on 2-D Von-Neumann Cellular Automata (VCA) dubbed IEVCA [28]. Gao et al. (2020) suggested combining Feistel architecture with short comparable encryption based on sliding window (SCESW) For edge computing security [29]. Jalal et al. (2020) presented Stable IoT coding technique. It uses a 64-bit block encryption key to encrypt data; a simple vocabulary comprising fundamental arithmetic operations may also be used [30]. Kiran V. and Shantharama C. (2021) proposed ARX/MRX, which stands for Addition Modulo/Multiplication Modulo, Rotation, and XOR. The cipher techniques employed reversible logic and Vedic Mathematics. It was implanted with reversible logic. It is based on Vedic mathematics and reversible logic [31]. Badr M. et al. (2021) proposed a lightweight cryptosystem for IoT devices with limited resources that uses AES and a novel chaotic S-box [32]. Zhang Y (2020) proposed image encryption algorithm uses a lifting algorithm by dividing the image into low- and high-frequency components. Chaos generates pseudorandom sequences and disrupts the two sets of features [33]. Mingwu Z et al. (2019) offer a large-scale image encryption technique. A hyperchaotic Chen system is calculated using SHA-512 and chaotic sequences. Then the image is permuted using pixel scrambling and cyclic shift. The XOR procedure also improves pixel correlation [34].

3. IoT system design

The confidentiality of IoT images is one of the most critical parts of IoT security that prevents unauthorized access and often delayed communications due to the additional operations used during the device process within the network.

Therefore, this paper proposed to deal with the trade-off between achieving a low correlation with the original image, including insufficient IoT computing resources. To build a lightweight image encryption algorithm, three essential components are required sensors, processors, and applications; each layer must have its properties to develop a proper IoT system, as shown in Fig. 1.

3.1 IoT sensor

The perception layer describes the front-end devices and the crucial structure sections of the IoT,also known as the sensor layer achieved in the bottom layer of IoT architecture; such sensors are gas, water quality, moisture.

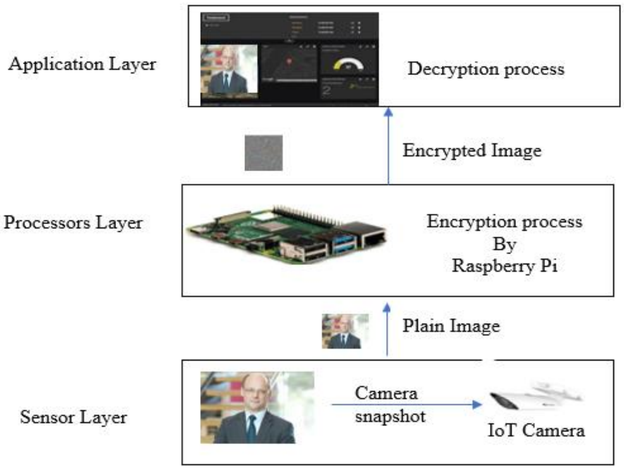

Figure. 1 The proposed IoT model

For machines and people to interpret these sensors' data, they must be converted into digital or analog signals. In the proposed architecture, an IoT camera is used in the IoT system to obtain images about the environment and dispatch them to the upper layer. To be easily recognizable over an extensive network, they should collect real-time data and have identifiable devices with an individual IP address.

3.2 IoT processors

Processors are the brain of every IoT system. Applications may operate processors to analyze received sensor data and extract relevant info from the vast raw data collected.

The second step in the IoT system is securing the receiving image from the camera connected with the Raspberry Pi device by performing the proposed chaotic encryption. It can process data since it has processors within. Arduino and Raspberry Pi are the most popular IoT gadgets.

Arduino is a single-purpose open-source platform microcontroller that links to a computer. Arduino boards can accept analog or digital data from sensors and convert it into an output, such as starting a motor, turning on/off LEDs, connecting to the internet, and more.

Raspberry Pi is a mini-computer with an OS sometimes known as the Raspbian operating system. It can run many programs at once. The Raspbian operating system is a free and open-source Linux alternative that keeps the Raspberry Pi's price low. The Raspberry Pi models are considered essential components of the IoT concept.

3.3 IoT application

This layer, known as the business layer, is created at the top of the IoT architecture. Many of the applications on this layer are used to offer cybersecurity to the end-user. The suggested chaotic algorithm is used in this layer to decrypt the received image before transmitting the plain image to the user.

4. The proposed image encryption scheme

One-dimensional maps have essential mathematical functions, a small key size, and an unsafe cryptosystem [35, 36]. Consequently, they are more vulnerable to assault than high-dimensional chaotic maps, which are more resistant and can survive attacks more effectively than one-dimensional maps [37]. Nevertheless, their implementation in hardware and software requires a significant amount of time to complete [38]. As a result, we adopt a two-dimensional Zaslavsky map to avoid the difficulties mentioned above and contain more parameters than a two-dimensional Henon map [39]. George M. Zaslavsky presented in 1978 Zaslavsky map is a two-dimensional dynamic system [40], which is defined as follows:

$$\begin{cases} y_{n+1} = y_n + v(1+\mu z_n)\varepsilon v\mu[\mathrm{Cos}(2\pi y_n)]Mod1 \\ z_{n+1} = e^{-\tau}[z_n + \varepsilon Cos(2\pi y_n)] \\ \mu \quad = \dfrac{1-e^{-\tau}}{\tau} \end{cases} \tag{1}$$

Where y and z are the two Zaslavsky sequences, whereas the variables ν, ε, and τ are the control parameters. When ν = 4, ε = 2.3 and τ = 3, the Zaslavsky map can reach a chaotic state. The chaotic attractor of the Zaslavsky map is explained in Fig. 2.

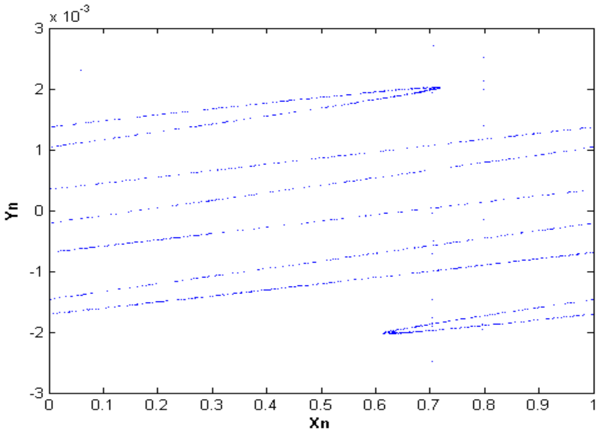

Figure. 2 The chaotic attractor of the Zaslavsky map

This section summarizes the key phases of the proposed method when starting values of the Zaslavsky map are determined by the values and locations of an input image and random values. We arrange ting matrices in ascending and descending order for permutation and diffusion operations after iterating the Zaslavsky map. Finally, the combined permutation-diffusion method is used to confuse and diffuse the image information concurrently as shown in Fig. 3.

The following are the major stages of the proposed encryption algorithm:

Step 1: Input the plaintext image PI (i,j) with size M × N, initial, values (X, Y) and control parameters of the Zaslavsky map (ν ε, and τ).

Step 2: Iterate the Zaslavsky map until the l M × N to avoid transit and generate e initial random matrices (D_1, D_2, and D_3).

Step 3: Update Zaslavsky map values (X_{MN}, Y_{MN}) based on initial random matrices (D_1, D_2, and D_3), pixel values PI (i,j), and pixel positions (i,j) to

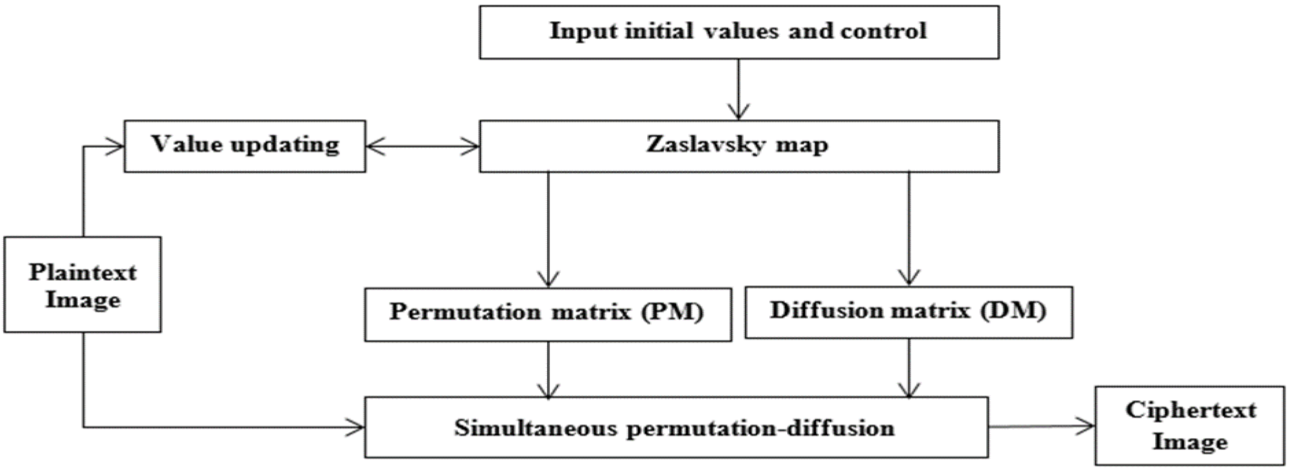

Figure. 3 The proposed encryption system

Received: January 16, 2022. Revised: February 18, 2022.

avoid a known-plaintext and chosen-plaintext attacks as follows:

$$F(PI) = \sum_{i=0}^{m} \sum_{j=0}^{n} \frac{D_1[i]}{D_2[j]} + \frac{D_3[PI(i,j)]}{M \times N \times 256} \quad (2)$$

$$\begin{cases} X_{MN+1} = X_{MN} + F\ Mod\ 1 \\ Y_{MN+1} = Y_{MN} + F\ Mod\ 1 \end{cases} \quad (3)$$

Step 4: Set the loop variable of the encryption round t=1.

Step 5: Continue Iterating the Zaslavsky map to generate two random matrices with M × N size: permutation matrix (PM) and diffusion matrix (DM).

Step 6: Sort the permutation matrix (PM) elements ascending and descending to get the index matrices of the ordered elements PM^a and PM^d, respectively.

Step 7: Obtain the diffusion matrix by normalizing the elements of DM as follows:

$$DM(i,j) = \lceil DM(i,j) \times 10^{14} \rceil Mod256 \quad (4)$$

Here $\lceil x \rceil$ is a mathematical function around the x to the nearest integer value.

Step 8: Beginning from the first to last row, we use Eq. (5) to permute and diffuse the image pixels (PI) simultaneously.

Where ⊕ denotes to XOR operation.

Step 9: Increase the loop variable of encryption round t=t+1.

Step 10: Return to step 5 until the encryption round T is reached.

The decryption procedure is achieved at the receiver side by reversing the stage of simultaneous permutation-diffusion as Eq. (6).

$$CI_{{PM^a}_{i,j},j} = \begin{cases} (DM_{i,j} \oplus (PI_{{PM^d}_{j,{PM^a}_{i,j}},{PM^a}_{i,j}} + PI_{{PM^a}_{M,N},N}))Mod\ 256\ \ IF\ i = 1\ and\ j = 1 \\ (DM_{i,j} \oplus (PI_{{PM^d}_{j,{PM^a}_{i,j}},{PM^a}_{i,j}} + CI_{{PM^a}_{i-1,N},N}))Mod\ 256\ \ IF\ i \neq 1\ and\ j = 1 \\ (DM_{i,j} \oplus (PI_{{PM^d}_{j,{PM^a}_{i,j}},{PM^a}_{i,j}} + CI_{{PM^a}_{i,j-1},j-1}))Mod\ 256\ \ IF\ j \neq 1 \end{cases} \quad (5)$$

$$PI_{{PM^d}_{j,{PM^a}_{i,j}},{PM^a}_{i,j}} = \begin{cases} (DM_{i,j} \oplus (CI_{{PM^a}_{i,j},j} - PI_{{PM^a}_{M,N},N}))Mod\ 256\ \ IF\ i = 1\ and\ j = 1 \\ (DM_{i,j} \oplus (CI_{{PM^a}_{i,j},j} - CI_{{PM^a}_{i-1,N},N}))Mod\ 256\ \ IF\ i \neq 1\ and\ j = 1 \\ (DM_{i,j} \oplus (CI_{{PM^a}_{i,j},j} - CI_{{PM^a}_{i,j-1},j-1}))Mod\ 256\ \ IF\ j \neq 1 \end{cases} \quad (6)$$

5. Experimental results and discussion

5.1 Histogram test

In the case of a digital image, an image histogram is a kind of histogram that serves as a graphical representation of the color distribution. The number of pixels is shown for each total value. A glance at the histogram reveals the whole tone distribution. This image histogram represents the RGB-level frequency. It is one of the most magnificent statistical vivid nesses of an image. After encryption, the histogram of the F-16 images, as shown in Fig. 4, confirmed that the presented method achieved an efficient result after encryption. In addition to the visual result, the distribution of pixels can be justified by a quantitative measure known as chi-square, defined by the following mathematical formula [41].

$$X^2 = \sum_{i=1}^{256} \frac{(P_i - E)}{E} \quad (7)$$

Where P_i and E represents the actual and anticipated numbers of each of the 256 gray level values in the image under test. The encrypted image passes the Chi-square measure if $X^2 < 293.2478$ at significance α =0.05. Table 1 reflects the success of the proposed image cryptosystem.

Table 1. Quantitative analysis of pixels distribution

Image	Original image	Encrypted image
F-16	822925.9603	259.4973
Mandrill	101863.4616	264.1074
Splash	951959.3021	271.3498
Peppers	340999.4414	260.8383
House	257525.5384	258.5586

5.2 Correlation coefficient analysis

The correlation between pixels is checked for statistical attacks and zero for optimal encryption.

The correlation is tested using random pairings of plain and encrypted images. Three thousand pairings are chosen randomly to verify the correlation coefficient using the following equations:[42]

$$E(x) = \frac{1}{N} \sum_{i=1}^{N} x_i \quad (8)$$

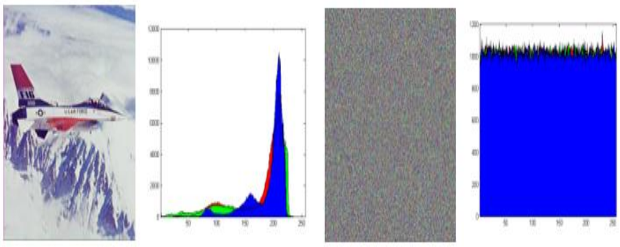

Figure. 4 Histogram test of F-16 image

Table 2. Correlation coefficients in different directions

no	Plaintext image			Ciphertext image		
	H	V	D	H	V	D
1	0.9758	0.9336	0.9199	0.0004	-0.0015	0.0002
2	0.9163	0.9505	0. 972	0.0014	0.0004	0.0007
3	0.9249	0.942	0.9655	0.0003	0.0012	-0.0023
4	0.9697	0.9172	0.9529	0.0008	0.0031	-0.0005
5	0.9556	0.9458	0.9181	-0.0021	0.0009	-0.0003

$$D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2 \qquad (9)$$

$$CC_{xy} = \frac{\frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y))}{\sqrt{D(x)}\sqrt{D(y)}} \qquad (10)$$

The total pixels designated by N, E(x), and E(y) are the mean values of x_i and y_i. The correlation coefficients of five imagers are shown in Table 2. The findings show that the encrypted images have low correlation coefficients. These correlation tests show that the image cryptosystem is near zero, preventing a statistical attack from yielding valuable information.

5.3 Shannon entropy analysis

Entropy is one of the most important works of the French mathematician Claude Shannon. In an image, it must be applied in each band of this depending on its type of color space. This test analyzes the histogram of the figure after it has been coded and determines if its frequency distribution is much more uniform than that of the original image. It is known that 255 is the maximum value of a pixel, and for its binary expression, it requires 8 bits; this implies that the perfect distribution of an image after being encrypted must be 8, which is unlikely to happen in practice. Therefore, any value greater than 7.9 indicates a high entropy level [43]. Eq. (11) calculates entropy.

Table 3. Global entropy test and local entropy test at k = 30, T_b= 1936 and a = 0.001

Image	F-16	Mandrill	Splash	Peppers	House
Global entropy	7.9998	7.9997	7.9998	7.9999	7.9986
Local entropy	7.9762	7.9684	7.9791	7.9695	7.9938

$$E(w) = \sum_{i=1}^{M} \mathrm{P}(z_i) \log_2 \mathrm{P}(z_i) \qquad (11)$$

Where $\mathrm{P}(z_i)$ represents the probability of message z_i and M is the total value of z_i. Wu et al. used local Shannon entropy over randomly selected k non-overlapping image blocks with fixed number of pixels (T_b) to overcome inaccuracy, inconsistency, and low efficiency problems in traditional entropy [44]. The local Shannon entropy is defined as:

$$\overline{E_{k,T_b}}(w) = \frac{1}{k}\sum_{i=1}^{k} E(w_i) \qquad (12)$$

Where $E(w_i)$ is the traditional entropy of non-overlapping image blocks w_i. For a significant image cryptosystem, the $\overline{E_{k,T_b}}(w) \in [7.9015, 7.9034]$ at k = 30 and $T_b =$ 1936 and confidence parameter a = 0.001. As reported in Table 3, the local entropy values of the encrypted image fall into an ideal interval that protects the output image of the proposed scheme against different statistical attacks.

5.4 Keyspace and key sensitivity

The secret keyspace is the size of the total of all variables utilized in the cryptosystem. To avoid brute-force attacks, the secret keyspace should be greater than 2^{100} [45]. For our proposed image cryptosystem, the secret keys are comprised of the initial values,y_0,z_0, ν, ε , τ and the encryption round T. Using the double-precision IEEE-754 standard, each initial value and control parameter of the Zaslavsky map will take10^{15}. Consequently, the total key size of the proposed method is around $(10^{15})^5 \approx 2^{250}$, which is more than 2^{100}, rendering brute-force attacks impossible.

One standard procedure for checking the sensitivities of these secret keys is to decipher the encrypted image with a key slightly modified by ΔCK (i.e., changing y_0 to $y_0 + \Delta\mathrm{CK}$ or $y_0 - \Delta\mathrm{CK}$). Then, the proposed scheme uses a ciphertext difference rate (CDR) test to verify the difference between the decrypted images and the original one in the proposed image encryption algorithm. This measure can be obtained by the following equations [46].

Table 4. Ciphertext difference rate (CDR) analysis of F-16 image for different secret keys CK with ΔCK = 10-15 for initial conditions and control parameters and ΔCK = 100 for idle iterations

Modified CK	CK value	CDR%
y_0	0.1	99.6873
z_0	0.1	99.5862
ν	4	99.7441
ε	2.3	99.685
τ	3	99.7038
T	12	99.6802

$$Diff\big(I_1(i,j), I_2(i,j)\big) = \begin{cases} 0 & IF\ I_1(i,j) = I_2(i,j) \\ 1 & IF\ I_1(i,j) \neq I_2(i,j) \end{cases} \tag{13}$$

$$DiffI(I_1, I_2) = \sum_{ij} Diff\big(I_1(i,j), I_2(i,j)\big) \tag{14}$$

$$CDR = \sum_{ij} \frac{DiffI(CI_1, CI_2) + DiffI(CI_1, CI_3)}{2 \times M \times N} \times 100\% \tag{15}$$

Where CI_1, CI_2 and $CI_3$are cipher images using different encryption keys CK, CK + ΔK, and CK −ΔCK, respectively. In general, having a CDR of more than 99% is considered a sufficient key sensitivity for an encryption scheme. To calculate CDR for the proposed scheme, the proposed algorithm modifies the entire secret key with a tiny change + ΔCK and –ΔCK on the F-16 image, as explained in Table 4. Based on the obtained results, it can be observed that the proposed cryptosystem provides a higher value of CDR. Hence, the proposed scheme performs well in the CDR measure.

5.5 Gray difference degree analysis

A gray difference degree (GDD) test is performed to examine the scrambling efficiency of the image encryption algorithm. To evaluate the GDD for the M×N image, first, we have to calculate the gray difference (GD) for all pixels except the pixels of the edges with the following expression:

$$GD(x,y) = \frac{\sum[I(x,y) - I(\overline{x},\overline{y})]^2}{4} \tag{16}$$

Where $\mathrm{I(x,y)}$ represents the gray value of image pixel, and $\mathrm{I}(\overline{\mathrm{x}},\overline{\mathrm{y}})$ is a gray value of four neighborhood pixels at $(\mathrm{x}+1,\mathrm{y})$, $(\mathrm{x}-1,\mathrm{y})$, $(\mathrm{x},\mathrm{y}+1)$ and $(\mathrm{x},\mathrm{y}-1)$ positions. After that, the result of a gray difference degree can be computed by using Eqs. (17) and (18).

$$E\big(GD(x,y)\big) = \frac{\sum_{x=2}^{M-1}\sum_{y=2}^{N-1} GD(X,Y)}{(M-2)(N-2)} \tag{17}$$

Table 5. GDD measures results and comparisons with other cryptosystems

Image	F-16	Mandrill	Splash	Peppers	House
GDD	7.9861	7.9924	7.9792	7.9868	7.9915

$$GDD = \frac{[\overline{O}(GD(X,Y)) - O(GD(X,Y))]}{[\overline{O}(GD(X,Y)) + O(GD(X,Y))]} \tag{18}$$

Where O and $\overline{\mathrm{O}}$ refer to the average neighborhood gray difference between plaintext images and the ciphertext images, respectively. A gray difference degree near one means that the cryptosystem is very difficult to reveal. As obtained from the comparison results in Table 5, the gray difference degree of the proposed algorithm is close to one, which means that there is a negligible relationship among original and encrypted images.

5.6 Resistance to differential attack

Most of the time, a cracker makes a modest modification to the pixels of the main image. It then utilizes the same encryption method to encrypt images comparable to the first. A plain image and an encrypted image are used in conjunction with this technique to determine the relationship. To determine whether or not the suggested method is resistant to differential assaults, we used the number of pixels change rate (NPCR) and the unified average changing intensity (UACI) metrics. The NPCR and UACI may be calculated using the formulae shown below:

$$V(i,j) = \begin{cases} 0 & IF\ CI_1(i,j) = CI_2(i,j) \\ 1 & IF\ CI_1(i,j) \neq CI_2(i,j) \end{cases} \tag{19}$$

$$NPCR = \sum_{ij} \frac{V(i,j)}{M \times N} \times 100\% \tag{20}$$

$$UACI = \sum_{ij} \frac{|CI_1(i,j) - CI_2(i,j)|}{255 \times M \times N} \tag{21}$$

Where $CI_1(i,j)$ and $CI_2(i,j)$ are the two encrypted images referring to the original image before and after a little modify; M and N determine the image length and width, respectively. The ideal NPCR and UACI depend on the image size and significance level α according to obtained results in [47], where the 512×512 gray image passe pass all theoretical NPCR critical values at significance level (α = 0.05), (α = 0.01) and (α = 0.001) if the result of $NPCR \geq 99.5893\%$. It passes the UACI test if the result within the critical interval of (33.3730%, 33.5541%), (33.3445%, 33.5826%) and (33.3115%, 33.6156%) at significance level (α = 0.05), (α = 0.01) and (α = 0.001), respectively. The results in

Table 6. Results of the NPCR measure

Images	NPCR%	α = 0.05	α = 0.01	α =0.001
		99.5893%	99.581%	99.5717%
F-16	99.7133	Succeed	Succeed	Succeed
Mandrill	99.6826	Succeed	Succeed	Succeed
Splash	99.7428	Succeed	Succeed	Succeed
Peppers	99.6937	Succeed	Succeed	Succeed
House	99.7053	Succeed	Succeed	Succeed

Table 7. Results of the UACI measure

Images	UACI	α=-0.05 33.373	α=- 0.01 33.3445	α=-0.001 33.3115
		α=+0.05 33.5541	α=+0.01 33.5826	α=+0.001 33.6156
F-16	33.4508	Succeed	Succeed	Succeed
Mandrill	33.5211	Succeed	Succeed	Succeed
Splash	33.5327	Succeed	Succeed	Succeed
Peppers	33.3809	Succeed	Succeed	Succeed
House	33.5295	Succeed	Succeed	Succeed

Table 6 and Table 7 demonstrate that the proposed cryptosystem is resistant to differential attacks.

5.7 Performance comparison

The performance of the suggested technique is compared to that of current schemes in Refs. [22, 23, 25-27, 30, 33]. Table 9 compares our method's keyspace, entropion, NPCR and UACI dominance on images to the prior techniques.

The suggested method's superiority is mostly due to its utilization of integrated confusion and diffusion processes, as well as unencrypted image information, for its starting states.

Compared to earlier cryptosystems, the proposed system efficient, has a higher performance, and can withstand contemporary assaults.

5.8 Analysis of running time

Encryption speed is critical for a safe IoT connection. Thus, comparing results from various algorithms in different contexts is challenging. For these reasons, the suggested cryptosystem's encryption speed is measured by Encryption Throughput (ET) and the Number of required Cycles per Byte (NCpB). Table 8 compares the proposed cryptosystem's encryption time, ET, and NCpB to existing cryptosystems in various situations. These results indicate that the proposed method is suitable for real-time image encryption.

Table 8. The speed analysis comparison results

Schemes	Encryption time (Unit: s)	ET	Megabytes per second	Cycles per byte
Proposed	0.3927	7.9114	1.9099	1099
Ref [22]	0.5101	1.4703	10.20	2500
Ref [23]	0.6093	0.3077	10.20	1099
Ref [25]	1.44	0.1302	1.2632	1550
Ref [26]	0.1098	6.8306	18.200	21511
Ref [27]	1.7815	0.421	0.2416	2500
Ref [30]	0.188	1.3297	0.9586	22
Ref [33]	2.423	7.9114	62.046	21511

Table 9. Performance comparison

Schemes	Key-space	Entropy	NPCR%	UACl%
Proposed	2^{250}	7.99723	99.7194	33.4635
Ref [22]	2^{250}	-	99.7133	33.4508
Ref [23]	2^{512}	7.99847	99.6094	29.2600
Ref [25]	2^{256}	7.99937	99.6455	33.4674
Ref [26]	2^{80}	7.9962	99.61	0.2821
Ref [27]	2^{128}	7.99932	99.6097	0.33455
Ref [30]	2^{128}	7.89	99.60	31.3394
Ref [33]	2^{256}	7.9981	-	-

6. Conclusion

The IoT development is expected to make more data and give people different information. IoT cameras are also becoming more popular, leading to many images being shared on social media and the internet every day. Healthcare and environmental monitoring use IoT to send images to the cloud without much human help. It is imperative to encrypt sensitive data before sending it over the internet.

This paper presents a chaotic system based on an integrated confusion-diffusion architecture to secure IoT images. Comparatively to other approaches to image encryption, this one changes the initial circumstances of the chaotic system to detect plaintext better. In order to minimize the association between close pixels, the created chaotic system was used to rearrange them in rows and columns.

The simultaneous confusion dispersion process ensures excellent security by mixing the encrypted pixels using metrics like chi-square, correlation, global and local Shannon entropy, local keyspace CDR encryption quality NPCR UACI and computational time analysis. These findings demonstrate the proposed system's excellent dependability, mean processing time, and resistance to current threats.

Conflicts of Interest

The authors declare that there is no conflict of interest.

Author Contributions

Conceptualization, Ahmed H., Ahmed K. and Mohammed H; methodology and implementation, Ahmed H., Ahmed K.; writing original draft preparation, Ahmed Hashim and Mohammed H.; writing, review and editing, Ahmed Hashim. and Ahmed K; supervision and funding acquisition, Ahmed Hashim, Ahmed K, and Mohammed H.

References

[1] Z. Guan, W. Yang, L. Zhu, L. Wu, and R. Wang, "Achieving adaptively secure data access control with privacy protection for lightweight IoT devices", *Science China Information Sciences*, Vol. 64, No. 6, pp. 1-14, 2021.

[2] D. Chattopadhyay and U. K. Ray, "A Scalable, Lightweight and Secure IoT Device Connector Service Using MQTT and ECC", *Lecture Notes in Networks and Systems*, Vol. 292, pp. 387-398, 2022.

[3] A. Fotovvat, G. M. E. Rahman, S. S. Vedaei, and K. A. Wahid, "Comparative Performance Analysis of Lightweight Cryptography Algorithms for IoT Sensor Nodes", *IEEE Internet of Things Journal*, Vol. 8, No. 10, pp. 8279-8290, 2021.

[4] A. Kumar and N. S. Raghava, "An efficient image encryption scheme using elementary cellular automata with novel permutation box", *Multimedia Tools and Applications*, Vol. 80, No. 14, pp. 21727-21750, 2021.

[5] J. Khan, J. P. Li, A. U. Haq, G. A. Khan, S. Ahmad, and A. A. Alghamdi, "Efficient secure surveillance on smart healthcare IoT system through cosine-transform encryption", *Journal of Intelligent and Fuzzy Systems*, Vol. 40, No. 1, pp. 1417-1442, 2021.

[6] M. G. Padmashree, S. Khanum, J. S. Arunalatha, and K. R. Venugopal, "ETPAC: ECC based trauma plight access control for healthcare Internet of Things", *International Journal of Information Technology*, Vol. 13, No. 4, pp. 1481-1494, 2021.

[7] Y. Sun, F. P. W. Lo, and B. Lo, "Light-weight Internet-of-Things Device Authentication, Encryption and Key Distribution using End-to-End Neural Cryptosystems", *IEEE Internet of Things Journal*, Vol. 14, No. 8, 2021.

[8] T. A. Idriss, H. A. Idriss, and M. A. Bayoumi, "A Lightweight PUF-Based Authentication Protocol Using Secret Pattern Recognition for Constrained IoT Devices", *IEEE Access*, Vol. 9, pp. 80546-80558, 2021.

[9] I. Sokol, P. Hubinský, and Ľ. Chovanec, "Lightweight cryptography for the encryption of data communication of iot devices", *Electronics*, Vol. 10, No. 21, 2021.

[10] B. M. Alshammari, R. Guesmi, T. Guesmi, H. Alsaif, and A. Alzamil, "Implementing a symmetric lightweight cryptosystem in highly constrained iot devices by using a chaotic s-box", *Symmetry*, Vol. 13, No. 1, pp. 1-20, 2021.

[11] G. Mishra, S. K. Pal, S. K. Murthy, K. Vats, and R. Raina, "Distinguishing lightweight block ciphers in encrypted images", *Defence Science Journal*, Vol. 71, No. 5, pp. 647-655, 2021.

[12] I. R. Chiadighikaobi and N. Katuk, "A scoping study on lightweight cryptography reviews in IoT", *Baghdad Science Journal*, Vol. 18, No. 2, pp. 989-1000, 2021.

[13] S. Ullah and R. Zahilah, "Curve25519 based lightweight end-to-end encryption in resource constrained autonomous 8-bit IoT devices", *Cybersecurity*, Vol. 4, No. 1, 2021.

[14] A. S. S. Thuluva, M. S. Somanathan, R. Somula, S. Sennan, and D. Burgos, "Secure and efficient transmission of data based on Caesar Cipher Algorithm for Sybil attack in IoT", *Eurasip Journal on Advances in Signal Processing*, Vol. 2021, No. 1, 2021.

[15] S. Nath, S. Som, and M. Negi, "LCA approach for Image Encryption Based on Chaos to Secure Multimedia Data in IoT", In: *Proc. of 2019 4th International Conference on Information Systems and Computer Networks*, pp. 410-416, 2019.

[16] L. Li, G. Wen, Z. Wang, and Y. Yang, "Efficient and Secure Image Communication System Based on Compressed Sensing for IoT Monitoring Applications", *IEEE Transactions on Multimedia*, Vol. 22, No. 1, pp. 82-95, 2020.

[17] A. Boutros, S. Hesham, B. Georgey, and M. A. A. E. Ghany, "Hardware acceleration of novel chaos-based image encryption for IoT applications", In: *Proc. of the International Conference on Microelectronics*, Vol. 2017-Decem, No. Icm, pp. 1-4, 2018.

[18] J. Ahmad, A. Tahir, J. S. Khan, M. A. Khan, F. A. Khan, Arshad, and Z. Habib, "A Partial Ligt-weight Image Encryption Scheme", *2019 UK/China Emerging Technologies*, pp. 1-3, 2019.

[19] M. Hoksbergen, J. Chan, G. Peko, and D. Sundaram, "Future Network Systems and Security", *CCIS. 2019*, Vol. 1113, 2019.

[20] S. K. Das, S. Samanta, N. Dey, and R. Kumar, “Design Frameworks for Wireless Networks”, Vol. 82, 2019.

[21] E. E. G. Guerrero, E. I. González, O. R. L. Bonilla, J. R. C. Valdez, and E. T. Cuautle, “Randomness improvement of chaotic maps for image encryption in a wireless communication scheme using PIC-microcontroller via Zigbee channels”, *Chaos, Solitons and Fractals*, Vol. 133, 2020.

[22] Y. Zhang, A. Chen, Y. Tang, J. Dang, and G. Wang, “Plaintext-related image encryption algorithm based on perceptron-like network”, *Information Sciences*, Vol. 526, pp. 180-202, 2020.

[23] Z. Hua, Z. Zhu, S. Yi, Z. Zhang, and H. Huang, “Cross-plane colour image encryption using a two-dimensional logistic tent modular map”, *Information Sciences*, Vol. 546, pp. 1063-1083, 2021.

[24] G. Cheng, C. Wang, and H. Chen, “A Novel Color Image Encryption Algorithm Based on Hyperchaotic System and Permutation-Diffusion Architecture”, *International Journal of Bifurcation and Chaos*, Vol. 29, No. 9, 2019.

[25] M. Gupta, K. K. Gupta, and P. K. Shukla, “Session key based fast, secure and lightweight image encryption algorithm”, *Multimedia Tools and Applications*, Vol. 80, No. 7, pp. 10391-10416, 2021.

[26] H. Liu, B. Zhao, J. Zou, L. Huang, and Y. Liu, “A Lightweight Image Encryption Algorithm Based on Message Passing and Chaotic Map”, *Security and Communication Networks*, Vol. 2020, 2020.

[27] S. Janakiraman, K. Thenmozhi, J. B. B. Rayappan, and R. Amirtharajan, “Lightweight chaotic image encryption algorithm for real-time embedded system: Implementation and analysis on 32-bit microcontroller”, *Microprocessors and Microsystems*, Vol. 56, pp. 1-12, 2018.

[28] S. Roy, M. Shrivastava, C. V. Pandey, S. K. Nayak, and U. Rawat, “IEVCA: An efficient image encryption technique for IoT applications using 2-D Von-Neumann cellular automata”, *Multimedia Tools and Applications*, Vol. 80, No. 21-23, pp. 31529-31567, 2021.

[29] R. Gao, S. Li, Y. Gao, and R. Guo, “A lightweight cryptographic algorithm for the transmission of images from road environments in self-driving”, *Cybersecurity*, Vol. 4, No. 1, 2021.

[30] M. J. Saddam, A. A. Ibrahim, and A. H. Mohammed, “A Lightweight Image Encryption and Blowfish Decryption for the Secure Internet of Things”, *4th International Symposium on Multidisciplinary Studies and Innovative Technologies*, 2020.

[31] K. V. G. Kiran and R. C. Shantharama, “FPGA implementation of a lightweight simple encryption scheme to secure IoT using novel key scheduling technique”, *International Journal of Applied Science and Engineering*, Vol. 18, No. 2, pp. 2-11, 2021.

[32] B. M. Alshammari, R. Guesmi, T. Guesmi, H. Alsaif, and A. Alzamil, “Implementing a symmetric lightweight cryptosystem in highly constrained iot devices by using a chaotic s-box”, *Symmetry*, Vol. 13, No. 1, pp. 1-20, 2021.

[33] Y. Zhang, “The fast image encryption algorithm based on lifting scheme and chaos”, *Information Sciences*, Vol. 520, pp. 177-194, 2020.

[34] M. Zhang, B. Peng, and Y. Chen, “An Efficient Image Encryption Scheme for Industrial Internet-of-Things Devices”, *IoT S and P 2019 - Proceedings of the 2nd International ACM Workshop on Security and Privacy for the Internet-of-Things*, pp. 38-43, 2019.

[35] S. Pan, J. Wei, and S. Hu, “A novel image encryption algorithm based on hybrid chaotic mapping and intelligent learning in financial security system”, *Multimed. Tools Appl.*, Vol. 79, No. 13, pp. 9163-9176, 2020.

[36] K. Suneja, S. Dua, and M. Dua, “A review of chaos based image encryption”, In: *Proc. of 2019 3rd International Conference on Computing Methodologies and Communication*, pp. 693-698, 2019.

[37] H. Wang, D. Xiao, X. Chen, and H. Huang, “Cryptanalysis and enhancements of image encryption using combination of the 1D chaotic map”, *Signal Processing*, Vol. 144, pp. 444-452, 2018.

[38] S. A. Mehdi and S. J. Muhamed, “Design and Analysis of a Novel Six-Dimensional Hyper Chaotic System”, *Al-Mustansiriyah J. Sci.*, Vol. 31, No. 4, pp. 62-71, 2020.

[39] M. H. Ahmed, A. K. Shibeeb, and F. H. Abbood, “An efficient confusion-diffusion structure for image encryption using plain image related Henon map”, *Int. J. Comput.*, Vol. 19, No. 3, pp. 464-473, 2020.

[40] G. M. Zaslavsky, “The simplest case of a strange attractor”, *Physics Letters A*, Vol. 69, No. 3, pp. 145-147, 1978.

[41] A. S. Mahmood and M. S. M. Rahim, “Novel method for image security system based on improved SCAN method and pixel rotation

technique", *Journal of Information Security and Applications*, Vol. 42, pp. 57-70, 2018.

[42] B. Arpacı, E. Kurt, K. Çelik, and B. Ciylan, "Colored Image Encryption and Decryption with a New Algorithm and a Hyperchaotic Electrical Circuit", *Journal of Electrical Engineering & Technology*, pp. 1-17, 2020.

[43] C. H. Lin, G. H. Hu, C. Y. Chan, and J. J. Yan, "Chaos-based synchronized dynamic keys and their application to image encryption with an improved aes algorithm", *Applied Sciences*, Vol. 11, No. 3, pp. 1-16, 2021.

[44] Y. Wu, Y. Zhou, G. Saveriades, S. Agaian, J. P. Noonan, and P. Natarajan, "Local Shannon entropy measure with statistical tests for image randomness", *Information Sciences*, Vol. 222, pp. 323-342, 2013.

[45] S. A. Banday, M. K. Pandit, and A. R. Khan, "Securing Medical Images via a Texture and Chaotic Key Framework", *Multimedia Security*, pp. 3-24, 2021.

[46] E. Yavuz, R. Yazıcı, M. C. Kasapbaşı, and E. Yamaç, "A chaos-based image encryption algorithm with simple logical functions", *Computers and Electrical Engineering*, Vol. 54, pp. 471-483, 2016.

[47] Y. Wu, J. P. Noonan, and S. Agaian, "NPCR and UACI randomness tests for image encryption", *Cyber Journals: Multidisciplinary Journals in Science and Technology, Journal of Selected Areas in Telecommunications*, Vol. 1, No. 2, pp. 31-38, 2011.