Journal of Theoretical and Applied Information Technology
15th August 2022. Vol.100. No 15

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

# LIGHTWEIGHT CHAOTIC BLOCK CIPHER FOR IOT APPLICATIONS

**MOUSA FARAJALLAH**
College of Information Technology and Computer Engineering, Palestine Polytechnic University, Hebron, Palestine
E-mail: mousa_math@ppu.edu

**ABSTRACT**

The Internet of Things is interrelated computing devices; each one has a unique identifier, one of the main advances of it the possibility of transfer data over the network without the need of human assistance. However, transfer data over the network susceptible to different types of attacks. The required encryption time of the classical encryption, techniques are not suitable to secure IoT data. This introduces the need for lightweight encryption algorithms in order to provide the required security level and decreasing the encryption time. In this paper a lightweight of one encryption round algorithm is proposed based on the Skew Tent Map. This map is used to produce the required confusion as well as diffusion effects to decrease the required encryption time to be used for real-time IoT applications. The obtained security analysis results confirm the high security level of the proposed algorithm. Moreover, the required encryption time comparing to the presented IoT encryption algorithm is less time. Encryption time and standard security analysis of the proposed cryptosystem confirms that this proposal is suitable for securing real-time applications.

**Keywords:** *IoT security, Skew Tent Map, Confusion, Diffusion, Image Encryption*

## 1. INTRODUCTION

Today, different kinds of communication channels have been used to transmit data, most of these channels are unsecured ones. As a result, huge work is devoted to develop cryptosystems to protect sensitive and critical information during transmission process [1]. IoT devices exchange data over network in order to complete their tasks. The exchange data in most of cases are plain and can be interrupted, read, and modify by any illegal user. Nevertheless, the required encryption time of the classical encryption method is not suitable for IoT applications.

Cryptosystems require a deterministic system producing the random or pseudo random behavior, this property one of the most powerful and important one in chaos theory. Using chaotic maps for encryption algorithms is new field of research that has been studied during last decade. The chaotic maps can be used as symmetric (the same key used for encryption and decryption) or asymmetric (two keys, the public is used for encryption and the private one for decryption in most cases) encryption algorithms [2]. Most of chaos-based encryption algorithms have been proposed for image and some of them for videos [3]– [9].

Researches have shown that chaos systems are extremely sensitive to the changes of control parameters and initial conditions. They have the pseudo-random behavior for non-authorized parties [3], [10]–[16]. Experimental results show that the chaos-based encryption algorithm achieves security purposes in an efficient and adaptive ways compared to the classical encryption algorithms (such as DES and AES) [17]–[22].

The basic properties of any secure system are confusion and diffusion, this has been stated in Shannon's paper [23] "In a strongly ideal cipher all statistics of the cryptogram are independent of the particular key used". In simple words, the target of using confusion layer is to increase the complexity relation between the secret key and the ciphered data/image. However, the secure system requires increasing the complexity relation between the plain-text/image and the cipher-text/image; this can be accomplished using the diffusion layer.

In [5], [6], Fridrich has proposed the first published chaos-based encryption algorithm. Three chaos-based maps are used to achieve the required

confusion level: Backer map, Cat map, and the Standard map. While a non-linear feedback register is used in order to achieve the required diffusion effect.

Masuda et al., [8], [9] presented two types of chaotic finite state maps: S-boxes and chaotic mixing transformation. They proposed block ciphers based on uniform and Feistel networks. In fact, they estimated bounds for the differential probability and the linear probability to make their cryptosystems resistant to differential and linear cryptanalysis. Since our cryptosystem based on a non-linear map used on this work, this map will be described in details in the next section.

Image encryption algorithm based on enhanced 1-D Chaotic was proposed in [4]. The proposed algorithm accomplishes substitution-permutation round *r* times. Two PWLCM maps are used: The first map is used during the substitution process to implement the addition modulo 256 and bit-wise operations. While the permutation process is achieved using the second map. Some of weakness of this algorithm are the error propagation caused by the used of perturbation technique and the slow encryption speed.

Yang et al., [24], presented an image encryption algorithm that includes the authentication property. In this scheme, 128 bits are generated from a hash algorithm while the input of this hash function are the secret hash keys and the plain image. The output (i.e., hash value) is used as a secret key during the encryption and the decryption processes. Furthermore, the hash secret key is used to authenticate the decrypted image. The permutation and substitution are performed in a single scan of the plain image pixels. The permutation process is achieved by the modified standard map and the substitution process (based on a logistic map). It is important to note that this algorithm depends on the plain-image to generate the secret key that is not recommended. Finally, in [25], fast and secure cryptosystems were proposed. To the best of our knowledge, these cryptosystems seem very secure, robust against attacks, and faster than the previous chaos-based cryptosystems. The cryptosystem results are used in security and execution time comparison with our proposed cryptosystem. However, Farajallah et.al presented a cryptanalysis model of this fast and secure algorithm in [26].

The rest of the paper is organized as follows: The most related works are presented in section **2**. The proposed cryptosystem is presented in **3**. Section **4** evaluate the time complexity and security robustness. Finally, conclusion is given in Section **5**.

## 2. RELATED WORK

In 1997, a chaos-based encryption scheme was introduced by Fridrich [5] [6]. It becomes the core structure of the most chaos-based cryptosystems and it is widely referenced since 1997. The general Fridrich architecture is shown in Figure-1 [27].

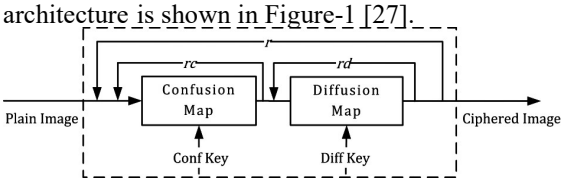



*Figure. 1. Fridrich Image Encryption Architecture*

The Fridrich encryption scheme includes two layers: The 2-D BAKER chaotic map to achieve the confusion effect. Where the second layer is based on equation 2. During the confusion layer, the 2-D chaotic map is used to calculate the new byte position using equation 1.

$$\begin{aligned} B(x,y) &= (2x, \tfrac{y}{2}) \quad when\ 0 \le x < \tfrac{1}{2} \\ B(x,y) &= (2x-1, \tfrac{y}{2}+\tfrac{1}{2}) \ when\ \tfrac{1}{2} \le x \le 1 \end{aligned} \tag{1}$$

$$\begin{aligned} v_k &= v_k + G(v_{k-1}) Mod\ 256 \\ v_{-1} &= initial\ value \end{aligned} \tag{2}$$

In the second layer, function G is some arbitrary function of the gray level which is implemented using a lookup table. In [28] Lian et al., the security of the Fridrich algorithm was evaluated and analyzed. They found some weaknesses, and they proposed some improvements of these security failures.

In 2010, Fridrich encryption algorithm has been broken by [29], Solak proves that the Fridrich algorithm can be broken using a chosen cipher-text attack. Using this type of attack, some secret permutation of the algorithm has been revealed.

In [9], a cryptosystem is introduced by Masuda et. al., this cryptosystem uses the modified Finite State Tent Map (FSTM) of equation 3 in the encryption side, and equation 4 in the decryption one, this encryption scheme is enhanced version of the one in [8].

$$F_A(X) = \begin{cases} \left\lfloor \frac{256}{A} \times X \right\rfloor + 1 & 1 \le X < A \\ 256 & X = A \\ \left\lfloor \frac{256 \times (256 - X)}{256 - A} \right\rfloor + 1 & A < X \le 256 \end{cases} \quad (3)$$

The inverse of 3 was calculated as:

$$F_A{}^{-1}(Y) = \begin{cases} X_1, & X_1 \times (256 - A) > A \times (256 - X_2) \\ X_2, & X_1 \times (256 - A) \le A \times (256 - X_2) \end{cases} \quad (4)$$

Where

$$X_1 = \left\lfloor \frac{A \times Y}{256} \right\rfloor \quad (5)$$

$$X_2 = 256 - \left\lfloor (1 - \frac{A}{256}) \times Y \right\rfloor \quad (6)$$

## 3. THE PROPOSED CRYPTOSYSTEM

The proposed research has based on research presented by Elassad et.al., [30] regarding the dependent confusion and diffusion with one round. Moreover, The Skew Tent Map analysis and weakness overcome is presented by Farajallah et.al., [27]. The proposed cryptosystem mode of operation is based on the Cipher-Block Chaining (CBC) mode [31]. When encryption based on block by block instead of encrypt the whole image it minimizes the total number of bits that are resulted from propagation error. The proposed cryptosystem uses our implementation of the chaotic generator that has been proposed by El Assad and Noura patent [32], the implementation produces a 32-bit samples. The general block diagram of any encryption scheme that uses CBC mod is shown in Figure.2.

$P_0$ is the first block from the plain image, IV is the initial vector, it is generated by the implemented chaotic generator, $C_0$ is the first ciphered block which will be transferred to the receiver side. The dash boxes represent the proposed encryption algorithm. This process is repeated for all blocks in the image.

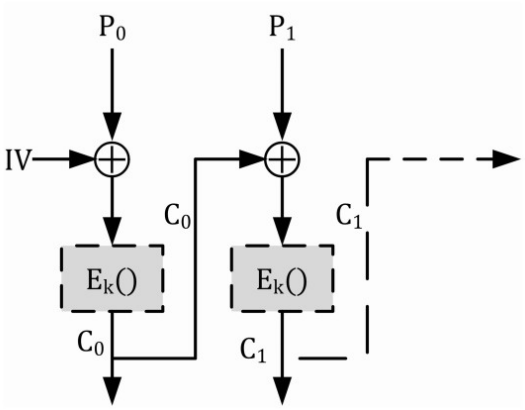



*Figure. 2. Encryption Based On CBC Mode*

### 3.1 Confusion Layer

The modified Skew tent Map in [33]is used to perform the permutation process.

$$F_A(X) = \begin{cases} (\left\lfloor \frac{Q}{A} \times (X+1) \right\rfloor + B) \ Mod \ Q & 0 \le X < A \\ (\left\lfloor \frac{Q \times (Q - X)}{Q - A} \right\rfloor + 1 + B) \ Mod \ Q & A \le X < Q \end{cases} \quad (7)$$

Where

$$\begin{aligned} A &\in \{1, 2, ...255\} \\ B &\in \{0, 1, 2....255\} \\ X &\in \{0, 1, 2....255\} \end{aligned} \quad (8)$$

In the previous equation 7, $A$ and $B$ are dynamic keys of 8 bits which are generated by the implementation of the used chaotic generator, these dynamic keys are changed four times inside the same block to increase the dynamic key space, $X$ is the pixel position in the block, $Q$ is the block size which is 256 in our proposed algorithm, $F_A(X)$ is the new position of the pixel. The MFSTM [33] is developed and designed to overcome the STM weaknesses and also to work as permutation layer for all positions between 0 and $Q$ – 1 inclusive.
In our proposed cryptosystem, the MFSTM is used as permutation layer to calculate the new pixel position from the old one and not as substitution layer. This technique decreases the time complexity while produce and distribute the required confusion effect.

### 3.2 Diffusion Layer

To use the MFSTM as a diffusion layer, it is not necessary to be invertible, and so the slow ceil operation can be replaced by the fast floor one:

$$G_{A_1}(X) = \begin{cases} \left(\left\lfloor \frac{255}{A_1} \times (X+1) \right\rfloor + B_1\right) Mod\ 255 & 0 \le X < A_1 \\ \left(\left\lfloor \frac{255 \times (255-X)}{255-A_1} \right\rfloor + 1 + B_1\right) Mod\ 255 & A_1 \le X < 255 \end{cases} \quad (9)$$

Where $A_1$, $B_1$ and $X$ in equation 9 has the same range as in equation 8. This generator is used as diffusion or substitution layer, the input value is $X$ and the new value is $G_{A1}(X)$. Algorithm-2.1 is proposed in order to achieve the both previous equation (diffusion and confusion) using the same encryption round to be used for real-time IoT applications.

### 3.3 Complete encryption scheme

The idea in this algorithm is not similar to that one used in most cryptosystems. Usually, the basic idea is to move or exchange the values between X and $F_A(X)$ in the permutation or swap process. In our proposed cryptosystem the encryption method based on transfer the diffusion and the confusion effects from the pixel at position X and the previous ciphered pixel (through the dynamic key generation process as presented in equation 11 to the pixel at position $F_A(X)$.

The proposed encryption scheme is designed to achieve the confusion and diffusion effects pixel by pixel instead of achieved them block by block or image by image. Wong applied this idea of sequential diffusion in his cryptosystem [34], which increases the spreading of one pixel effect to the all next pixels; the general block diagram of the proposed cryptosystem is shown in Figure.3. The cryptosystem is designed such as the required security level is achieved from the first encryption round. Algorithm summarizes the encryption process.

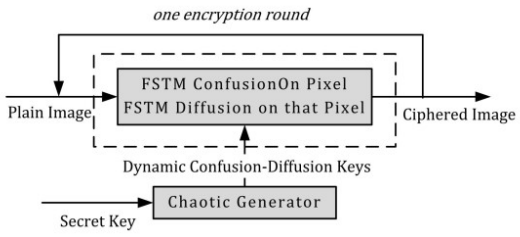



Figure. 3. General Block Diagram Of The Proposed Image Encryption Scheme

In the decryption side, equations 11 and 12 are used to retrieve the original plain pixel from the ciphered pixel as:

$$P(X) = C(F_A(X)) \oplus Key \quad (12)$$

where $P(X)$ is the plain pixel at position $X$, $C(F_A(X))$ is the ciphered pixel at position $F_A(X)$, $Key$ is the dummy variable used to transfer confusion and diffusion effects, the input value of the generator at the first pixel (i.e $C(F_A(-1))$ is derived from the implementation of the used chaotic generator.

**Algorithm 3.1**

(1) Take 8 bit $X$ from the chaotic generator and calculate the $G_{A_1}(X)$ using (9).
(2) Set $X = 0$ and $key = G_{A_1}(X)$, calculate $C(F_A(X))$ using (10).
(3) Increment $X$ by one position.
(4) Calculate $Key$ using (11).
(5) Calculate $C(F_A(X))$ using (10).
(6) If $X$ value less than the block size go to step 3.
(7) The encryption equation is:

### 3.4 Complexity And Security Analysis

NIST (National Institute of Standards and Technology) has proposed three types of criterions in order to evaluate any proposed cryptographic algorithms: - Security, Cost and Implementation characteristics [48-49] those criteria have been validated in sections 2.2.2 to section 2.2.8. in addition to section 2.3.

First of all, the complexity of any proposed cryptosystem is important evaluation factor, since the lightweight cryptosystem is proposed for IoT applications. Traditionally, in most research papers, this factor is evaluated by measuring the encryption/decryption time. In the next section this measurement tool is used. However, new complexity measurements are used, which are throughput, and number of cycles are required to encrypt/decrypt one byte. Second, some theoretical security analyses are presented. Finally, the common experimental and statistical analysis is used to test the robustness of the proposed cryptosystem for all kinds of known attacks in the literature.

#### 3.4.1 Complexity analysis

The process of calculating the execution time of the encryption and decryption processes of our proposed cryptosystem is carried out using a GCC compiler of the C programming, on a PC with 3.1 GHz processor Intel ® Core ™ i3-2100 CPU, 4GB RAM, and Windows 7, 32-Bit operation System. The image under the test was gray and color Lena image of different sizes (256×256×3, 512×512×3 and 1024×1024×3). The calculated time is compared with fastest IoT and real-time cryptosystems. From Table I, it is clear that our proposed cryptosystems are faster than all cryptosystem in the literature. Table II presents the

encryption throughput (running speed) in MBps (Mega Byte Per Second) and the number of cycles that are required to encrypt/decrypt one byte. The encryption throughput is calculated by equation 13 in bytes. While equation 14 is used to calculate the number of cycles that needed to encrypt one byte.

*Table 1: Encryption/Decryption Time Of Different Algorithms(In Milli-Second)*

| | 256 | 512 | 1024 |
|---|---|---|---|
| Proposed | 2.8/2.9 | 11.12/11.25 | 46.1/46.2 |
| khan 2020 (IoT) [35] | 10.2 | 28.1 | 123.9 |
| muhammad 2018 (IoT) [36] | 16.1 | 67.1 | 282.1 |
| Qumsieh 2019 [37] | 4.6 | 18.06 | 54.35 |
| Zhang 1 [25] | 7.5/7.5 | 30/30 | 120/120 |
| Zhang 2 [25] | 7.5/8.25 | 30/33 | 120/132 |
| Wang [38] | 7.79/8.39 | 31.16/33.54 | 124.64/134. |
| Akhshani [11] | 14.4 | 57.6 | 230.4 |
| Wong [34] | 15.59/16.77 | 62.37/67.11 | 249.48/268. |
| Kanso [39] | 97.15 | 388 | 1554 |

$$ET = \frac{Image_{Size}(Byte)}{Encryption_{Time}(second)} \quad (13)$$

$$\text{Number of cycles per Byte} = \frac{\text{CPU Speed}_{(Hertz)}}{ET_{(Byte)}} \quad (14)$$

*Table 2: Encryption Throughput And Number Of Cycles For One Ciphered Byte*

| | ET in MBps | Number of cycles per byte |
|---|---|---|
| Proposed | 66.9/64.65 | 44.17/45.72 |
| khan 2020 (IoT) [35] | 1.89 | 1625 |
| muhammad 2018 (IoT) [36] | 1.3 | NA |
| Qumsieh 2019 [37] | 41.52 | 62 |
| Zhang 1 [25] | 25/25 | 122.07/122.07 |
| Zhang 2 [25] | 25/22.72 | 122.07/134.27 |
| Wang [38] | 24.06/22.35 | 122.85/132.24 |
| Akhshani [11] | 13.02 | 194.83 |
| Wong [34] | 12.03/11.18 | 245.7/264.38 |
| Kanso [39] | 1.93 | 1121 |

From Tables (I-II), it is clear that our proposed cryptosystem faster than both IoT and chaos-based cryptosystems. However, the encryption speed is not sufficient to evaluate the cryptosystem. Since any proposed cryptosystem shall have high security level beside the fast encryption and decryption speed.

### 3.4.2 Known plain-text attack

Fridrich proved that his proposed model is secure against known plain-text attack based on the fact that the difference between the cipher-texts encrypted by the same key for two plain-texts differs on one bit is large enough to keep a high security level against the known plain-text attack. However, Lian in [28] pointed out another known plain-text attack that can be used to cryptanalyze the Fridrich model. Since the fixed point problem was not solved in the 2-D cat map, Baker or standard maps were used in the Fridrich model, and so the cipher of the first plain pixel of any image will remain in the first position (that means $c_0$ is the encryption of the $p_0$, and so, no permutation is done on the first pixel). Then it is easy to find the initial value of the diffusion key ($Q_1$) in the Fridrich model (more details of this attack are in [28]).

To overcome this drawback, Zhang et. al. presented a simple solution by swapping between a random pixel in the image and the top-left pixel. On the other hand, in the Zhang cryptosystem, some ciphered pixels have limitations on mapping to all possible values. For instance, the $ciph(1; 0)$ can only come from the plain pixel at $arr(1; q_1)$, where arr is the plaintext array, $q_1$ is the used dynamic key in Zhang cryptosystem.

In our proposed cryptosystem, the first kind of known plaintext attack is solved, and it satisfies a high security level. This is well stated by our proposed cryptosystem in section (2.2.4). The second kind of known plain-text attack does not exist in our proposed cryptosystem, since the fixed-point problem is solved by adding the $B$ and the $B_1$ dynamic keys to the original FSTM as a generator and also as a substitution map. Our solution has two advantages, first, it increases the dynamic key space of the FSTM. Second, any pixel can be mapped to any position with the same probability.

### 3.4.3 Plain-text Sensitivity Attacks

The sensitivity of any cryptosystem to one bit change in the plain-text is important to resist the known plain-text and the chosen plain-text attacks [28] [40]. The test scenario to evaluate the sensitivity of the proposed cryptosystem is: Two plain-text $P_1$ and $P_2$(with one bit differs between them) are selected to encrypt them using the same secret key, to analyze the difference between their corresponding ciphertexts. In most research papers, the different bit between $P_1$ and $P_2$ is the first bit in the image. However, in our proposed cryptosystem, this bit is chosen to be located in the beginning, middle and the end of the first block, the plain-text results are calculated as an average of these three cases). The security parameters are used to measure the resistance of any proposed cryptosystem

regarding the plain-text sensitivity attacks are: The Number of Pixels Change Rate (NPCR) and the Unified Average Changing Intensity (UACI), they are given by the following equations respectively:

$$NPCR = \frac{1}{L \times C \times P} \times \sum_{p=1}^{P} \sum_{i=1}^{L} \sum_{j=1}^{C} D(i,j,p) \times 100\% \quad (15)$$

where

$$D(i,j,p) = \begin{cases} 0, & \text{if} \quad C_1(i,j,p) = C_2(i,j,p) \\ 1, & \text{if} \quad C_1(i,j,p) \neq C_2(i,j,p) \end{cases} \quad (16)$$

$$UACI = \frac{1}{L \times C \times P \times 255} \times \sum_{p=1}^{P} \sum_{i=1}^{L} \sum_{j=1}^{C} |C_1 - C_2| \times 100\% \quad (17)$$

The optimal NPCR value is 99.61%, and the optimal UACI value is 33.46% [41] [42]. These tests are used in general to evaluate any propose algorithm regarding differential attacks introduced by Eli Biham and Adi Shamir [43]. The previous tests are important but not sufficient to be sure that the proposed cryptosystem is secure against the plaintext sensitivity attacks. A new measurement test is called Avalanche effect is used. The output of the system should be changed significantly (50% of the output should be changed) when a single bit change on the input [44]. The scenario of this test is exactly similar to the previous one, but here the Hamming distance is used to evaluate the cryptosystem if it has the Avalanche effect or not:

$$HD(C_1, C_2) = \frac{1}{|Ib|} \sum_{K=1}^{|Ib|} (C_1(K) \oplus C_2(K)) \quad (18)$$

The scenario of testing the proposed cryptosystem for plaintext attacks when the different bit is the first one is shown in Figure.4. The Hamming distance (HD) between the corresponding ciphered images C1 and C2 should be closed to 50% (probability of bit changes). Therefore, the plain-text sensitivity attack would become useless attacking method. Table III presents results of the previous tests for different image based on different sizes (the image type and image sizes are chosen to be similar to that one in the compared cryptosystems). In that table it is clear that the *HD* value is too close to the optimal one. The *UACI* and *NPCR* values are also too close to the optimal.

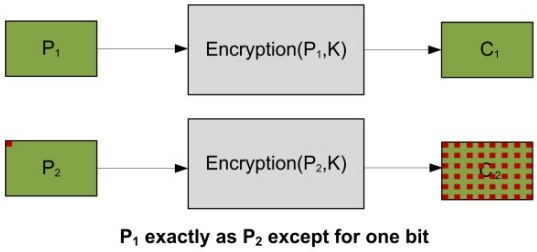



*Figure. 4. Plain-Text Sensitivity Attack Scenario*

All values in that table indicate that the proposed cryptosystem is very sensitive to one-bit change in the plain-text. Hence, a high security level is reached.

*Table 3: Hd, Uaci And Npcr Plain-Text Sensitivity Tests*

| | Image | size | HD | UACI | NPCR |
|---|---|---|---|---|---|
| Proposed | Barb | 512, Gray | 0.499999 | 33.488 | 99.626 |
| Zhang 1 [25] | Barb | 512, Gray | / | 33.475 | 99.663 |
| Zhang 2 [25] | Barb | 512, Gray | / | 33.420 | 99.582 |
| Proposed | Lena | 512, Gray | 0.499997 | 33.475 | 99.618 |
| Qumsieh 2019 [37] | Lena | 512, Gray | 0.499354 | 33.431 | 99.513 |
| Wong [34] | Lena | 512, Gray | / | 32.82 | 99.44 |
| Wang [38] | Lena | 512, Gray | / | 33.435 | 99.607 |
| Ahmed [17] | Lena | 512, Gray | / | 33.4 | 99.6 |
| Proposed | Boat | 256, Gray | 0.499998 | 33.484 | 99.629 |
| Song [45] | Boat | 256, Gray | / | 33.453 | 99.625 |
| Akhshani [11] | Boat | 256, Gray | 0.499900 | 33.200 | - |
| Proposed | lena | 512, Color | 0.499999 | 33.471 | 99.613 |
| khan 2020 (IoT) [35] | lena | 512, Color | *NA* | 33.602 | 99.629 |
| muhammad 2018 (IoT) [36] | lena | 512, Color | *NA* | 33.495 | 99.628 |
| Kanso [39] | lena | 512, Color | / | 33.44 | 99.610 |
| ECKBA [46] | lena | 512, Color | / | 33.36 | 99.612 |

### 3.4.4 Key Sensitivity Attack

The second type of sensitivity attacks is based on one bit different in the secret key, any cryptosystem should resist this type of sensitivity attacks. It is almost similar to the key sensitivity attacks scenario. A slight change in the secret key should produce a completely different ciphered image, and then the cryptosystem has a high security level relative to the key sensitivity attacks. The testing scenario of the key sensitivity is almost similar to the plain-text sensitivity attacks test as follows: Only one plain-text $P$ is required, two secret keys differ in one bit ($K_1$; $K_2$). First, $P$ is encrypted using $K_1$ to obtain $C_1$. Then the same plain-text $P$ is encrypted using $K_2$ to obtain $C_2$. The previous equations of the *NPCR*, *UACI* and *HD* (15, 17 and 18) are used to evaluate the key sensitivity attacks of the proposed cryptosystem. The scenario of evaluating key sensitivity attacks is shown in Figure.5. Table IV presents the average results of the key sensitivity attacks of the proposed cryptosystem using the same parameters were used in Table III.

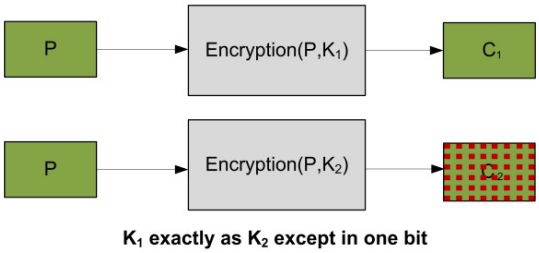



*Figure. 5. Plain-Text Sensitivity Attack Scenario*

From Table IV, the proposed cryptosystem has high security level relative to the key sensitivity attacks which confirms the robustness of the proposed cryptosystem regarding the sensitivity-based attacks.

*Table 4: Hd, Uaci And Npcr Key-Text Sensitivity Tests*

| | Image | HD | UACI | NPCR |
|---|---|---|---|---|
| Proposed | Lena 512 color | 0.499999 | 33.488 | 99.612 |
| Proposed | Barb 512 gray | 0.499991 | 33.481 | 99.601 |
| Proposed | Boat 512 gray | 0.499989 | 33.461 | 99.609 |

### 3.4.5 Histogram Analysis

To resist one of important attacks based on statistical analysis, the histogram of the ciphered image should be uniformly distributed. Figure-6 shows a) the plain-image, b) the corresponding cipher image, c) the histogram of the plain image, and d) its corresponding histogram of the ciphered image. It can be observed that the ciphered image histogram is close to the uniform distribution and so there is no visual or statistical information can be observed from the ciphered image. To statistically confirm the uniformity of the ciphered image histogram, chi-square test is applied (see equation 19).

$$\chi^2_{exp} = \sum_{i=0}^{Nv-1} \frac{(o_i - e_i)^2}{e_i} \quad (19)$$

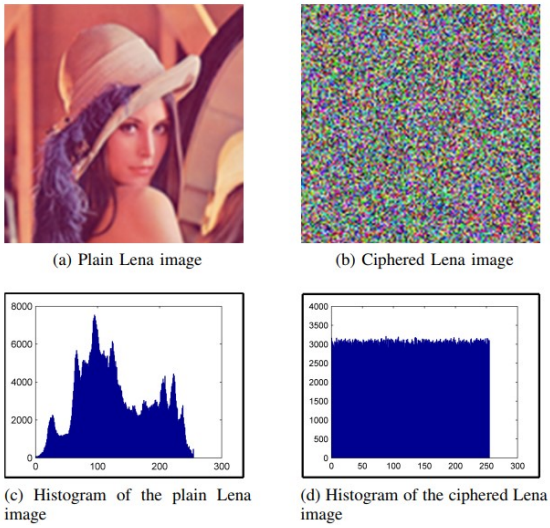
Where $N_v$ is the number of levels (here 256), $o_i$ is the observed occurrence frequencies of each color level (0-255) on the histogram of the ciphered image, and $e_i$ is the expected occurrence frequency of the uniform distribution, given here by $e_i = L \times 256\ C \times P$. The obtained result is presented in Table V. These results of the Chi square test are taken from histograms of three ciphered images of different natures (i.e., Lena, Boat, and Baboon) having the size of 128×128×3, with a significant level of 0.05. The obtained values in that table meet the condition

$$\chi^2_{exp} < \chi^2_{th}(255, 0.05) = 293$$

Then the tested histograms are uniform and do not reveal any information for the statistical analysis.

### 3.4.6 Correlation Analysis

The ciphered image should be greatly different from its plain one. One of measurement tools to evaluate this critical and required property is the correlation analysis.



(a) Plain Lena image (b) Ciphered Lena image

(c) Histogram of the plain Lena image (d) Histogram of the ciphered Lena image

*Figure. 6. Lena Image And Ciphered Lena And Their Histograms*

In fact, it is well known that adjacent pixels in the plain images are very redundant and correlated. So, in the ciphered images, adjacent pixels should have a redundancy and a correlation as low as possible.

*Table 5: Chi-Square Results*

| Ciphered image | Chi-square |
|---|---|
| Lena | 251.27 |
| Boat | 2657.46 |
| Baboon | 247.915 |

To perform the correlation test between two adjacent pixels, the following procedure was carried out. Firstly, 10000 pairs of two adjacent pixels are selected randomly in vertical, horizontal, and diagonal directions from the plain-image as well as the corresponding ciphered one. Then, the correlation coefficient was computed according to the following formulas:

$$\rho_{xy} = \frac{cov(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \quad (20)$$

Where

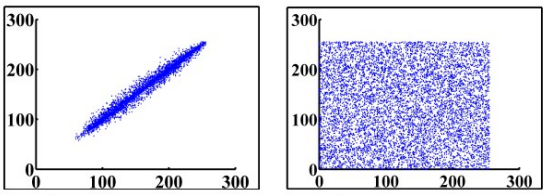
$$cov(x,y) = \frac{1}{N}\sum_{i=1}^{N}([x_i - E(x)][y_i - E(y)]) \quad (21)$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2 \quad (22)$$

$$E(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i) \quad (23)$$

*Table 6: Correlation Analysis Results*

| Crypto Name | Horizontal | Vertical | Diagonal |
|---|---|---|---|
| Proposed Algorithm | 0.0085 | 0.0097 | 0.0092 |
| Zhang 1 [25] | −0.0082 | −0.0004 | 0.0013 |
| Zhang 2 [25] | 0.0009 | −0.0027 | 0.0015 |
| khan 2020 (IoT) [35] | 0.0030 | 0.0018 | 0.0052 |
| muhammad 2018 (IoT) [36] | 0.0035 | 0.0055 | 0.0081 |




(a) Horizontal correlation of the plain image (b) Horizontal correlation of the ciphered image

*Figure. 7. Correlation Analysis Of Lena And It's Ciphered Image In Three Directions*

*N*=10000 is the sample size, while *x* and *y* are the gray-level values of the two adjacent pixels in the image. The test image is a Lena gray scale image of 512×512×3. The obtained results are shown in Table VI and Figure.7. These results demonstrate that the correlation coefficient, in all directions, of the plain-text images is close to one, whereas the correlation coefficient of the ciphered images is close to zero. This means there is no detectable correlation exists between the original and its corresponding ciphered image. Subsub section has to be in sentense case with no spacing above or blow the srat of it.

### 3.4.7 Measurement of encryption quality

This measurement is introduced first by [47], it evaluates the difference between the frequency of the pixel value before and after the encryption, as this difference is higher as the encryption quality is better, to summarize this new security measurement tool, the following pseudo code is presented.

**Algorithm 3.2**

Initialize $i = 0$.
Declare and initialize arrays $(P, C)$ of 256 element to 0.
Set $IS$ to be the image size.
  While($i < IS$)
    Read the plain pixel at position $i$ and save it in $x$.
    Read the ciphered pixel at position $i$ and save it in $y$.
    Increment the $P$ value at position $x$ by $P[x] + +$.
    Increment the $C$ value at position $y$ by $C[y] + +$.
    Increment the counter $i$.
  End While
Initialize $i = 0$.
Initialize the encryption quality $EQ = 0$.
  While($i < 256$)
    Update the $EQ$ by $EQ = EQ + abs(P[i] - C[i])$.
    Increment the counter $i$.
  End While
Calculate the Final $EQ$ by $EQ = \frac{EQ}{256}$.
Calculate the percentage of $EQ$ by $EQ = \frac{EQ}{TS}$.

The optimal value for RC5 and RC6 in [47] is 721, our proposed cryptosystem produce a close value for the same test image (Lena gray scale image of 512 × 512) which is 673, this value with previous security tests guarantee the high security level of our proposed cryptosystem.

## 4. CONCLUSION

The modified FSTM is used in novel scenario in order to speedup the computation time as well as enhance the security level. The proposed chaotic cryptoystem is fast, simple, and robust against known attacks for secure image and data transmissions over network for IoT applications. The proposed structure is formed by a diffusion layer based on a modified FSTM for a substitution function and it is well-known that FSTM has a high non-linearity property. The confusion layer is achieved using the same modified map but for a permutation function during the key generation. The time evaluation section ensures that the proposed cryptosystem is faster than all IoT and chaosbased cryptosystems in the literature. The security analysis of the obtained experimental results shows that the proposed cryptosystem is resistant to all attacks identified in the literature. One of the most important results of the proposed cryptosystem that it requires only one iteration to provide sufficient security level. Moreover, the proposed algorithm is suitable for hardware implementation and it is convenient for IoT real time applications. Finally, this algorithm is suitable for lightweight IoT applications that required medium security level and very fast encryption

speed. While for high security level this algorithm is not sufficient.

## REFERENCES:

[1] S.-F. Hsiao, M.-C. Chen, and C.-S. Tu, "Memory-free low-cost designs of advanced encryption standard using common subexpression elim ination for subfunctions in transformations," Circuits and Systems I: Regular Papers, IEEE Transactions on, vol. 53, no. 3, pp. 615–626, 2006.

[2] R. Tenny and L. S. Tsimring, "Additive mixing modulation for public key encryption based on distributed dynamics," Circuits and Systems I: Regular Papers, IEEE Transactions on, vol. 52, no. 3, pp. 672–679, 2005.

[3] G. Chen, Y. Mao, and C. K. Chui, "A symmetric image encryption scheme based on 3d chaotic cat maps," Chaos, Solitons & Fractals, vol. 21, no. 3, pp. 749–761, 2004.

[4] D. Socek, S. Li, S. S.Maglivera, and B. Furht, "Short paper: Enhanced 1-d chaotic key based algorithm for image encryption, sep. 2005."

[5] J. Fridrich, "Symmetric ciphers based on two-dimensional chaotic maps," International Journal of Bifurcation and Chaos, vol. 8, no. 06, pp. 1259–1284, 1998.

[6] ——, "Image encryption based on chaotic maps," in Systems, Man, and Cybernetics, 1997. Computational Cybernetics and Simulation., 1997 IEEE International Conference on, vol. 2. IEEE, 1997, pp. 1105–1110.

[7] L. Zhang, X. Liao, and X. Wang, "An image encryption approach based on chaotic maps," Chaos, Solitons & Fractals, vol. 24, no. 3, pp. 759– 765, 2005.

[8] N. Masuda and K. Aihara, "Cryptosystems with discretized chaotic maps," Circuits and Systems I: Fundamental Theory and Applications, IEEE Transactions on, vol. 49, no. 1, pp. 28–40, 2002.

[9] N. Masuda, G. Jakimoski, K. Aihara, and L. Kocarev, "Chaotic block ciphers: from theory to practical algorithms," Circuits and Systems I: Regular Papers

[10] L. O. Chua, M. Hasler, J. Neirynck, and P. Verburgh, "Dynamics of a piecewise-linear resonant circuit," Circuits and Systems, IEEE Transactions on, vol. 29, no. 8, pp. 535–547, 1982.

[11] A. Akhshani, A. Akhavan, S.-C. Lim, and Z. Hassan, "An image encryption scheme based on quantum logistic map," Communications in Nonlinear Science and Numerical Simulation, vol. 17, no. 12, pp. 4653–4661, 2012.

[12] M. Farajallah, S. El Assad, and M. Chetto, "Dynamic adjustment of the chaos-based security in real-time energy harvesting sensors," in Green Computing and Communications (GreenCom), 2013 IEEE and Internet of Things (iThings/CPSCom), IEEE International Conference on and IEEE Cyber, Physical and Social Computing, Aug 2013, pp. 282–289.

[13] F. Salam, J. Marsden, and P. P. Varaiya, "Chaos and arnold diffusion in dynamical systems," Circuits and Systems, IEEE Transactions on, vol. 30, no. 9, pp. 697–708, 1983.

[14] F. Chiaraluce, L. Ciccarelli, E. Gambi, P. Pierleoni, and M. Reginelli, "A new chaotic algorithm for video encryption," Consumer Electronics, IEEE Transactions on, vol. 48, no. 4, pp. 838–844, 2002.

[15] S. Behnia, A. Akhshani, H. Mahmodi, and A. Akhavan, "A novel algorithm for image encryption based on mixture of chaotic maps," Chaos, Solitons & Fractals, vol. 35, no. 2, pp. 408–419, 2008.

[16] G. M. Bernstein and M. A. Lieberman, "Secure random number generation using chaotic circuits," Circuits and Systems, IEEE Transactions on, vol. 37, no. 9, pp. 1157–1164, 1990.

[17] A. A. Abd El-Latif, X. Niu, and M. Amin, "A new image cipher in time and frequency domains," Optics Communications, vol. 285, no. 21, pp. 4241–4251, 2012.

[18] B. Furht and D. Socek, "Multimedia security: Encryption techniques," IEC Comprehensive Report on Information Security, pp. 335–349, 2003.

[19] S. Li, G. Chen, and X. Zheng, "Chaos-based encryption for digital image and video," Multimedia Encryption and Authentication Techniques and Applications, p. 129, 2006.

[20] G. J.-I and Y. J.-C, "A new chaotic key-based design for image encryption and decryption," in Circuits and Systems, 2000. Proceedings. ISCAS 2000 Geneva. The 2000 IEEE International Symposium on, vol. 4. IEEE, 2000, pp. 49–52.

[21] B. Bhargava, C. Shi, and S.-Y. Wang, "Mpeg video encryption algo rithms," Multimedia Tools and Applications, vol. 24, no. 1, pp. 57–79, 2004.

[22] I. Mansour, G. Chalhoub, and B. Bakhache, "Evaluation of a fast symmetric cryptographic algorithm based on the chaos theory for wireless sensor networks," in Trust, Security and Privacy in Computing and Communications (TrustCom), 2012 IEEE 11th International Conference on. IEEE, 2012, pp. 913–919.

[23] C. E. Shannon, "Communication theory of secrecy systems," Bell system technical journal, vol. 28, no. 4, pp. 656–715, 1949.

[24] H. Yang, K.-W. Wong, X. Liao, W. Zhang, and P. Wei, "A fast image encryption and authentication scheme based on chaotic maps," Communications in Nonlinear Science and Numerical Simulation, vol. 15, no. 11, pp. 3507–3517, 2010.

[25] W. Zhang, K.-w. Wong, H. Yu, and Z.-l. Zhu, "An image encryption scheme using reverse 2-dimensional chaotic map and dependent diffusion," Communications in Nonlinear Science and Numerical Simulation, 2013.

[26] M. Farajallah, S. El Assad, and O. Deforges, "Cryptanalyzing an image encryption scheme using reverse 2-dimensional chaotic map and dependent diffusion," Multimedia Tools and Applications, vol. 77, no. 21, pp. 28 225–28 248, 2018.

[27] M. Farajallah, S. El Assad, and D. Olivier, "Fast and secure chaos-based cryptosystem for images," International Journal of Bifurcation and Chaos, vol. 26, no. 02, p. 1650021, 2016.

[28] S. Lian, J. Sun, and Z. Wang, "Security analysis of a chaos-based image encryption algorithm," Physica A: Statistical Mechanics and its Applications, vol. 351, no. 2, pp. 645–661, 2005.

[29] E. Solak, C. Çokal, O. T. Yildiz, and T. Biyikoglu, "Cryptanalysis of ˘ fridrich's chaotic image encryption," International Journal of Bifurcation and Chaos, vol. 20, no. 05, pp. 1405–1413, 2010.

[30] S. El Assad and M. Farajallah, "A new chaos-based image encryption system," Signal Processing: Image Communication, vol. 41, pp. 144– 157, 2016.

[31] W. F. Ehrsam, C. H. Meyer, J. L. Smith, and W. L. Tuchman, "Message verification and transmission error detection by block chaining," Feb. 14 1978, uS Patent 4,074,066.

[32] S. EL ASSAD and H. NOURA, "Generator of chaotic sequences and corresponding generating system," Oct. 7 2011, wO Patent 2,011,121,218.

[33] M. Farajallah, "Chaos-based crypto and joint crypto-compression systems for images and videos," Ph.D. dissertation, Universite de Nantes, 2015.

[34] K.-W. Wong, B. S.-H. Kwok, and W.-S. Law, "A fast image encryption scheme based on chaotic standard map," Physics Letters A, vol. 372, no. 15, pp. 2645–2652, 2008.

[35] J. Khan, J. P. Li, B. Ahamad, S. Parveen, A. U. Haq, G. A. Khan, and A. K. Sangaiah, "Smsh: Secure surveillance mechanism on smart healthcare iot system with probabilistic image encryption," IEEE Access, vol. 8, pp. 15 747–15 767, 2020.

[36] K. Muhammad, R. Hamza, J. Ahmad, J. Lloret, H. Wang, and S. W. Baik, "Secure surveillance framework for iot systems using probabilistic image encryption," IEEE Transactions on Industrial Informatics, vol. 14, no. 8, pp. 3679–3689, 2018.

[37] R. Qumsieh, M. Farajallah, and R. Hamamreh, "Joint block and stream cipher based on a modified skew tent map," Multimedia Tools and Applications, vol. 78, no. 23, pp. 33 527–33 547, 2019.

[38] Y. Wang, K.-W. Wong, X. Liao, and G. Chen, "A new chaos-based fast image encryption algorithm," Applied soft computing, vol. 11, no. 1, pp. 514–522, 2011.

[39] A. Kanso and M. Ghebleh, "A novel image encryption algorithm based on a 3D chaotic map," Communications in Nonlinear Science and Numerical Simulation, vol. 17, no. 7, pp. 2943–2959, 2012.

[40] Y. Mao, G. Chen, and S. Lian, "A novel fast image encryption scheme based on 3d chaotic baker maps," International Journal of Bifurcation and Chaos, vol. 14, no. 10, pp. 3613–3624, 2004.

[41] 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 (JSAT), pp. 31–38, 2011.

[42] F. Maleki, A. Mohades, S. M. Hashemi, and M. E. Shiri, "An image encryption system by cellular automata with memory," in Availability, Reliability and Security, 2008. ARES 08. Third International Conference on. IEEE, 2008, pp. 1266–1271.

[43]E. Biham and A. Shamir, "Differential cryptanalysis of des-like cryp tosystems,"

Journal of CRYPTOLOGY, vol. 4, no. 1, pp. 3–72, 1991.

[44] P. P. Mar and K. M. Latt, "New analysis methods on strict avalanche criterion of s-boxes," World Academy of Science, Engineering and Technology, vol. 48, pp. 150–154, 2008.

[45] C.-Y. Song, Y.-L. Qiao, and X.-Z. Zhang, "An image encryption scheme based on new spatiotemporal chaos," Optik-International Journal for Light and Electron Optics, 2012.

[46] D. Socek, S. Li, S. Magliveras, and B. Furht, "Short paper: Enhanced 1-d chaotic key-based algorithm for image encryption," in Security and Privacy for Emerging Areas in Communications Networks, 2005. SecureComm 2005. First International Conference on, Sept 2005, pp. 406–407.

[47] H. E. H. Ahmed, H. M. Kalash, and O. Allah, "Encryption efficiency analysis and security evaluation of rc6 block cipher for digital images," in Electrical Engineering, 2007. ICEE '07. International Conference on, April 2007, pp. 1–7. IV-G.

[48] Murphy, Sean. "The power of NIST's statistical testing of AES candidates." Preprint. January 17 (2000): 118.

[49] Farajallah, Mousa, et al. "Selective Encryption of the Versatile Video Coding Standard." IEEE Access 10 (2022): 21821-21835.