Multimedia Tools and Applications
https://doi.org/10.1007/s11042-019-08112-z

Joint block and stream cipher based on a modified skew tent map

Rawan Qumsieh[1] · Mousa Farajallah[2] · Rushdi Hamamreh[3]

Received: 28 July 2018 / Revised: 21 June 2019 / Accepted: 13 August 2019 /
Published online: 29 August 2019

Abstract

Image encryption is very different from that of texts due to the bulk data capacity and the high redundancy of images. Thus, traditional methods are difficult to use for image encryption as their pseudo-random sequences have small space. Chaotic cryptography use chaos theory in specific systems working such as computing algorithms to accomplish dissimilar cryptographic tasks in a cryptosystem with a fast throughput. For higher security, encryption is the approach to guard information and prevent its leakage. In this paper, a hybrid encryption scheme that combines both stream and block ciphering algorithms is proposed in order to achieve the required level of security with the minimum encryption time. This scheme is based on an improved mathematical model to cover the defects in the previous discredited model proposed by Masuda. The proposed chaos-based cryptosystem uses the improved Skew Tent Map (STM) $RQ\text{-}FSTM$ as a substitution layer. This map is based on a lookup table to overcome various problems, such as the fixed point, the key space restrictions, and the limitation of mapping between plain text and cipher text. It uses the same map as a generator to change the byte position to achieve the required confusion and diffusion effects. This modification improves the security level of the original STM. The robustness of the proposed cryptosystem is proven by the performance and the security analysis, as well as the high encryption speed. Depending on the results of the security analysis the proposed system has a better dynamic key space than previous ones using STM, a double encryption quality and a better security analysis than others in the literature with speed convenience to real-time applications.

Keywords Stream cipher · Block cipher · Finite State Tent Map · Cryptosystem

1 Introduction

Chaos theory is the study of the behavior of dynamical systems that are very sensitive to initial conditions. Started at first in mathematics [53, 57], then has been developed

✉ Mousa Farajallah
mousa_math@ppu.edu

Extended author information available on the last page of the article.

by many other research areas including physics, chemistry and biology [40, 52, 71]. Despite the fact that these dynamical systems are based on deterministic models, their high sensitivity to initial conditions or control parameters cause their outputs to be unpredictable. The beginning of the chaotic systems returns back to the 1880's by Henry Poincare in his attempt to prove the stability of the solar system through his work on the restricted three-body problem [63]. Later, Edward Lorenz in 1961 contributed to the chaos theory [35].

One of the interesting applications of chaos is in the field of cryptography, as it concerns about techniques to secure the transfer of messages between two ends by encrypting those messages. Thus, many researchers have highlighted the strong relationship between chaos and cryptography [19, 20, 29]. More interestingly, Shannon indicated in his paper:"Communication Theory of Secrecy Systems" that was published in 1949 [56], that good transformation in good secrecy systems is achieved by basic operations that are the heart of chaotic maps [33]. In the same paper, Shannon invented two terms that are considered the major concepts of block ciphers, namely "confusion" and "diffusion", where the mixing property and sensitivity to initial conditions of chaos generators are mapped to the diffusion and confusion of cryptosystems. Hence, the tight relationship between chaos and cryptography, created a new field of research called chaotic cryptography, where a lot of work has been published [10, 21, 22, 32, 39, 59, 65].

Chaos was used in the two types of modern encryption, which are symmetric-key encryption in its both forms, the stream ciphers and the block ciphers, and public-key encryption. In stream ciphers, the chaos generators are used to generate a stream of pseudo-random numbers in which researchers used as keys to mask the plaintext as in [37, 50, 62]. On the other hand, in block ciphers, the key is used as an initial conditions and the control parameters of the chaos generators which then generates the cipher text after many encryption rounds as the image encryption block cipher proposed in [27, 70].

This paper is mainly to improve the core mathematical model of a chaos-based cryptosystem designed by Masuda's model [37], where many researchers have been using since 2002. Throughout the years, and after focusing on the chaos-based cryptosystems during the last decade, Masuda's model became a discredited model as the researchers showed many weaknesses in the model such as [13]. Thus, the improvement of Masuda's mathematical model is required to obtain a more robust model that will give us a better security level than the previous models with a faster cryptosystem. Masuda's model was improved to give a better key space, a robust model against theoretical attacks, and a more uniformly distributed domain. Later, the cryptosystem is tested against theoretical and statistical attacks where the robustness of the proposed cryptosystem was proven by the performance and security analysis. This paper is organized as follows: Section 2 presents the literature review of the similar presented works. In Section 3, the proposed cryptosystem and contribution is described in detail. Section 4 presents the security analysis. Where Section 5 concludes the proposed work.

2 Literature review

Zhang et al., present a fast chaos based cryptosystems [72], the presented cryptosystems mainly based on Fridrich's architecture [17], it depends on two layers, the first layer is used to achieve the diffusion effect and the second layer for confusion effect. However, Farajallah et al., present a partially cryptanalyzed method of Zhang cryptosystem [14] .

Implementation of an image encryption scheme based on the quantum logistic map is presented by Akhshani et al. [3]. The presented cryptosystem is based on one quantum logistic map using three steps: initialize the key and the plainimage, then the image is transformed into one dimensional array, finally, the map is used to encrypt the array content using the derived key. The presented cryptosystem has a good security results where the execution time is not appropriate for fast and real-time applications.

One of the most related work of the proposed cryptosystem is presented by Wang et al. [64]. In the presented cryptosystem, the both permutation and diffusion steps are combined together in order to decrease the encryption time. Moreover, the obtained security level is high for sensitive applications.

Farajallah et al. proposed a chaos based cryptosystem based on independent three chaotic maps, the obtained security results are satisfying the requirements of the real-time harvesting sensors, where as the encryption time is acceptable [15].

Kanso et al. [28] presented a chaos based cryptosystem using three dimensional chaotic maps that can defeat the sensitivity attacks. The design of the presented algorithm is simple and efficient and it achieves the required confusion and diffusion properties.

Pareek et al. [47], present a modified version of [46], in the modified version a multiple one-dimensional chaotic maps are used instead of only a one-dimensional chaotic map. The presented work divides the plaintext into variable block size, which are encrypted randomly. However, the encryption time of Pareek et al. cryptosystem is not appropriate for real-time or IoT applications.

Wong et al., [67] presented a fast chaos cryptosystem based on standard chaotic map. The structure of the presented cryptosystem consists such that the required diffusion effect is achieved in the substitution stage by simple sequential add-and-shift operations. The obtained security results and the execution time is proved the robustness and speed of this cryptosystem for secure real-time applications.

Chunhu et al., [31] presented up to date image encryption scheme based on 3D Chaotic logistic map. The first step is to generate the secret key using a modified 3D chaotic logistic map. Then use the same maps to encrypt the image with modification to improve the security level. The presented work is satisfying the security requirement. However, the execution time is not appropriate even for offline applications and it is clear the lower level of encryption throughput.

In 2019, Xu et al., [69] presents a high speed image encryption algorithm based on compressive sensing and hyperchaotic map. It is based on a new 2D sine improved logistic iterative chaotic map. The presented results show that the algorithm has high security level, good compression factor and high speed encryption. In fact, the execution time is slower than the most presented work in the literature review.

Matthews suggested the first chaotic encryption algorithm in 1989 [39]. Later, researches on chaos-based encryption increased, Baptista [4] completed one of these primary studies. A simple one-dimensional logistic map was used to encrypt each character of a text message as the integer number of iterations achieved in the logistic equation.

Jakimoski and Kocarev [26] attempted to examine Baptista cryptosystem and concluded that it has two imperfections; the encryption speed is average in correlation with other cryptosystems due to essential number of iterations, on the other hand, this system is not robust to known-plaintext attacks, however, it was the outset of using chaos theory in cryptography.

The authors of [58], present a review of image encryption techniques based on chaotic systems, the try to group the chaotic image encryption into spatial and frequency domain,

where in spatial domain, the presented chaotic based cryptosystems deal with images values in normal method. However, in a frequency domain, they deal with the rate at which the pixel values are changing in a spatial domain. The presented review concludes that a high security level cryptosystem should be based on using hybrid chaotic techniques.

Fredric in 1997 [17, 18] proposed the first chaos-based image cryptography. Researchers focused more on chaotic image encryption by using different chaotic maps to overcome the traditional cryptosystem disadvantages, and it worth telling that this technique was a sufficient way for image encryption due to the speed and the strong security.

On the other hand, the authors of [5] used a one-dimensional chaotic equation alternative map that can be used for twofold image encryption with the probability of consuming a huge number of keys. Later, Z. Han et al. in [24] proposed a non-linear map which was used for duplicating pixel values. Where the authors of [1] utilized three different chaotic maps for image encryption. The authors spread a 2D cat map on 8×8 blocks of an image to achieve the shuffling of the pixels and used the 2D coupled logistic map to produce control parameters of shuffling. Later the shuffled image is encrypted by 1D Logistic map; thus, there was no data leakage from encrypted image.

A three encryption algorithms named as Triple-Key chaotic proposed by [61] in 2011. Those keys are an initial parameter key, 80-bit session key and control parameter key. The work was a combination between [48] and [55] which focus around the logistic chaotic map and chaotic neural network.

In 2013, the authors of [25] proposed a classical cryptosystem that focuses on the AES and the chaotic logistic map to analyze the security eligibility of both cryptosystems and to evaluate the speed of both algorithms. The AES algorithm offered a better security performance in this study, but was slower regarding the encryption running speed. On the other hand, because of the computational cost, and the easiness of implementation the logistic map is more substitute for image encryption in real-time correspondence.

Murillo-Escobar et al. in [44] presented a color image encryption algorithm based on the plain image characteristics to resist a chosen and known plain image attack, and a 1D logistic map with to get a faster encryption process based on Murillo-Escobar's algorithm [43]. Dimensional chaotic maps have some drawbacks to be used in encryption as their data distribution is not uniform, their periodicity is relatively short, and have small key space. Thus, the authors used the 1D logistic map, as it has many powerful advantages such as the simple structure and the ease of implementation, and they are ideal for fast encryption.

Rafik et al. [41, 51] presented a privacy-preserving cryptosystem for IoT E-healthcare applications. The presented cryptosystem includes a new Pseudo Random Number Generator (PRNG). It is based on cascading the orbits of two of the 2D chaotic maps and produce the encryption keys for the cryptosystem algorithm. The presented PRNG is tested and evaluated to be used in cryptography applications.

Finally, the work in [8] is based on a chaotic system and deoxyribonucleic acid (DNA) sequence. The plain image is converted to a DNA matrix, and the chaotic map are used to generate a key matrix that is used to merge the confused DNA matrix; and then the initial values and system parameters of the chaotic system are updated by the hamming distance of the plain image and finally decoded the diffused DNA matrix, to get the ciphered image.

3 Proposed cryptosystem

3.1 Overview

The Finite State Tent Map (FSTM) mathematical model was introduced by Masuda et al. in [37, 38] as shown in (1):

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

where

$$X_1 = \left\lfloor \frac{A \times Y}{256} \right\rfloor \tag{2}$$

and

$$X_2 = 256 - \left\lfloor (1 - \frac{A}{256}) \times Y \right\rfloor \tag{3}$$

Q here is the block size, and it is equal to 256. And $X, A, Y \in \{1, 2, 3...Q\}$.

This version excluded the value 0, therefore, some authors tried to shift the model to include 0 and exclude Q from the range of X, A and Y (the plaintext, the key and the ciphertext). Still, this model had many drawbacks, such as the division by zero when A = Q, and some values of the output decreases the probability of guessing the value of the input [13]. As a result, Masuda's model became a discredited version of the FSTM, where the last updated model was modified by [13], where $X, Y \in \{0, 1, 2, 3...Q\}$, $A \in \{1, 2, 3...Q\}$ and $Q = 256$ as in (4):

$$F_A(X) = \begin{cases} \left\lceil \frac{Q}{A} \times (X+1) \right\rceil mod\, Q & 0 \le X < A \\ \left\lfloor \frac{Q \times (Q-X)}{Q-A} \right\rfloor + 1 mod\, Q & A \le X < Q \end{cases} \tag{4}$$

3.2 Proposed equation

Depending on the study of (1), and its improvement in [13], an extra part was added to the first interval of the equation to make sure that the domain will be more distributed in the proposed equation, as the domain of the output in (1) is concentrated around several values. The proposed mathematical model became as in (5)

$$R_Q(X) = \begin{cases} \left\lceil \frac{Q}{A(X-1)} + \frac{Q(A+1)}{X} \right\rceil mod\, Q & 0 \le X < A \\ \left\lfloor \frac{Q \times (Q-X)}{\frac{1.5}{Q-A}} \right\rfloor mod\, Q & A \le X < Q \end{cases} \tag{5}$$

where $X, Y, A \in \{0, 1, 2, 3...Q-1\}$ and $Q = 257$.

The encryption quality and the information entropy are calculated for the proposed model after every single change until the best results. During the experiment, the values increased regularly till the point "$\frac{Q(A+1)}{X}$", where at that point the increasing process is stopped to avoid any loss of information from the image. The middle interval of Masuda's equation

was deleted to guarantee not having the same result when A is equal to X. Those changes were done to obtain the following:

1. **A better key space**

   After studying the range of the key space in [13, 37],it is important to note that the only active bits in the key space are 66 odd values out of the 256, which makes it weak, as for some values it's easy to guess the input value. On the other hand, the model doesn't reach the perfect secrecy, as the key space is not equal to the plaintext space and not equal to the ciphertext space as well, which is proposed in their model to be equal to 256.

   In number theory, a and b are said to be relatively prime, or co-prime if the only positive integer that divides both of them is one. Thus, their greatest common divisor being 1 [7]. To increase the security level of the model, A and Q have to be co-prime. Pointing to the models of [13, 37], when Q=1, with $X, Y, A \in \{0, 1, 2, 3...Q\}$.

   The key space will contain only: $A = \{51, 53, 55, ..., 117, 139, 141, 143, ..., 201\}$ that are the cop-rime to 256 that counts 66 active bits in the key space.

   Following the same concept, Q is suggested to be 257 instead of 256 to increase the security level. Depending on the fact that 257 is a prime number, $A \in \{0, 1, 2, 3...Q - 1\}$ will give us 256 active bits in the keys space as all the numbers under 257 are co-prime with it, which at the same time will decrease the probability of guessing any input from the output value.
2. **A secure model against theoretical attacks**

   Masuda's model had an interval that made it easy to make the possibilities less when guessing the input value. As the output is always 256 when X=A. Thus, by increasing the possibilities of guessing the output, the cryptosystem is considered more robust against the theoretical attacks. Depending on that point, X=A is merged to the second interval of the proposed mathematical model.
3. **To have a more uniformly distributed domain**

   The strength of the cryptosystem's output is directly proportional to the distribution of its domain. As the main goal is to obtain a stronger core model for the chaotic systems, the model in [13] is changed to be as distributed as possible. Depending on the evaluation of the results, the proposed model gave a better distribution domain than the previous models of Masuda [37], and Farajallah [13]. The result of the information entropy analysis and the encryption quality analysis that are shown in the section of the security analysis, shows that the proposed system has a better-distributed domain than the previous models – the nearer to the uniformly distributed domain among others.

3.3 Cryptosystem design

The proposed cryptosystem is based on a hybrid encryption scheme that combines both stream and block ciphering algorithms to achieve the required security level, with a minimum encryption time. Both stream and block ciphers in cryptography belong to the family of symmetric key ciphers in which the same key is used for both of the encryption and the decryption processes.

The stream cipher converts the plaintext bits directly into the ciphertext by XORing them with pseudo-random cipher bits, while block cipher encrypts fixed size blocks that contain a group of bits from the plaintext [66]. The stream cipher has a higher speed of transformation and a low error rate, as an error that occurs in one bit will not affect the other bit. The block cipher has a high level of diffusion which any block effect will be spread into several blocks.

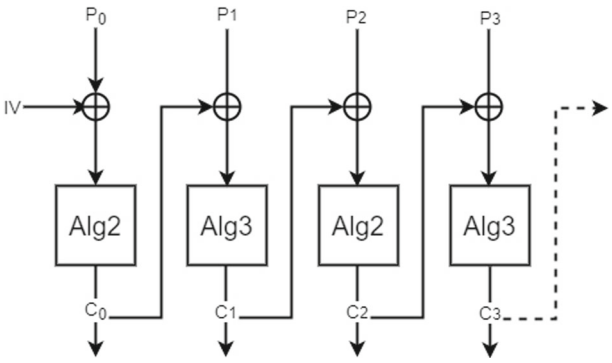


Fig. 1 The proposed algorithm encryption process

On the other hand, the diffusion effect is low in the stream cipher, as all information of the plaintext is contained in a single ciphertext symbol. The block cipher has low encryption speed, as the entire block must be accumulated before the encryption or decryption process starts. Furthermore, the entire block may be corrupt due to an error in one bit.

In the proposed cryptosystem, the image is divided into several numbers of blocks with a block size of 256 bytes and encrypted it block by block to minimize the error bits. As shown in Fig. 1, using the Cipher-Block Chaining (CBC) mode in the proposed cryptosystems, which is a confidentiality mode as it chains (combine) the plaintext block with the previous ciphertext block. The CBC mode requires an initialization vector to combine it with the first plaintext block which is generated in the proposed system by the chaotic generator.

In Fig. 1, P_0 represents the first plain block, the IV is the initial vector that is generated by El Assad generator [12], and C_0 is the ciphered block.

The proposed algorithm encrypts the whole image using Alg_2 and Alg_3 shown in Fig. 1, it encrypts the odd and the even blocks using different algorithms as shown in Fig. 2.

Alg_2 encrypts the odd blocks based on the proposed model R_Q-FSTM as shown in Fig. 3. Where as the substitution and the permutation are done in one step to decrease the encryption time. . First of all, the new position is calculated from the old one based on the proposed FSTM, then the permutation is achieved when the posn is used instead of the old position. In addition, the same equation is used in order to achieve the substitution by xoring the old value with the key. Finally, the key value is updated using the proposed FSTM but with different values of the updated process of the new position.

Alg_3 encrypts the even blocks as shown in Fig. 4 using a selective substitution based on R_Q-FSTM to decrease the time and to increase the encryption quality at the same time. It is similar to Alg_2, but only the most 2 significant bits of the byte at the new position is xored with the 2 least significant bits of the key.

Algorithm 1: Encryption Process
Divide image into n blocks 1- For odd blocks call Algorithm 2 2- For even blocks call Algorithm 3

Fig. 2 Algorithm 1: the encryption process

Algorithm 2: Odd Blocks

For i=0: 1 to Block size
1- Calculate the new position of the block (posn)
2- Permutation and substitution for data at posn
Block [j][posn]=Block[j][i]⊕Key
3- Update the Key
Key=lookup(Key, Block[j][posn])
End i

Fig. 3 Algorithm 2: odd block encryption

Afterward, the diffusion and confusion effects in the proposed cryptosystem are transferred between blocks using the CBC mode [11]. Its worth telling as well, that the model (5) was implemented based on a look-up table to decrease the encryption time. The input of this look-up table is the generated dynamic key from the implemented version of El Assad et al. [12] chaotic generator, in addition to the byte from the plaintext.

El Assad chaotic generator was implemented to avoid the weakness in the chaotic systems regarding periodicity-generating sequences. This generator consists of two chaotic maps, i.e., the Skew Tent Map (STM) and the discrete Piece-Wise Linear Chaotic Map (PWLCM), in which are connected in parallel to generate the sequence values of 32-bit samples [16].

4 Security analysis

To design and develop a chaos-based cryptosystem, the system should be suitable and efficient for the target application, achieve the degree of the security level, and not to consume time or memory. It should offer the required security level. Analyzing the complexity of any cryptosystem is an important assessment factor. Researchers typically take this evaluation as the time of encryption/decryption, however, measure that is more comprehensive are needed to evaluate the cryptosystem. In this section, the whole security analysis for Masuda [37], Farajallah [13] and the proposed cryptosystem results are reproduced.

Algorithm 3: Even Blocks

For i=0: 1 to Block size
1- Calculate the new position of the block (posn)
2- Perform permutation and selective substitution for data at posn
DataByte[j][posn]= the most 2 significant bits of the
DataByte[j][posn] ⊕ the least 2 significant bits of the dynamic key
3- Update the Key
Key=lookup(Key, Block[j][posn])
End i

Fig. 4 Algorithm 3: even block encryption

4.1 Theoretical analysis

4.1.1 Key space

Resisting the brute force attack needs a large secret key, with at least 128 effective and independent bits. Depending on that fact, the proposed proposed cryptosystem is robust against the brute force attack as it has a secret key with 169 bits which was calculated using two chaotic maps: the discrete STM and the discrete PWLCM [16]. And a dynamic key that consists out of 8 bits that are changeable and unique for each new block, and have been chosen out of 257 active values.

4.1.2 Ciphertext only attack

In this theoretical attack, a group of ciphertexts are available to the attackers, where they try to find the corresponding plaintexts. Where the complexity to resist such an attack is based on the available amount of the ciphertexts. This type of attack is facilitated when the attacker has multiple pieces of ciphertext generated from the same key which is not existed in the proposed model.

4.2 Differential cryptanalysis

Differential cryptanalysis is presented by Biham and Shamir for the first time to be used in Data Encryption Standard (DES) [6]. It is used in order to analyze how much a small change in the plaintext effect the corresponding ciphertext. This analysis can be used to partially or completely cryptanalyze the cryptosystem under the test. To measure this change effect two common parameters are used: The Unified Average Changing Intensity (UACI), and the Number of Pixels Change Rate (NPCR) [36, 68].

4.2.1 Plaintext sensitivity attack

Depending on the diffusion definition, any slight change in the plain image, even a change of a single bit, should statistically, change one bit out of two of the cipher image, and similarly, if one bit of the cipher image is flipped, then approximately one half of the plain image bits should change.

$$UACI = \frac{1}{L \times C \times P \times 255} \times \sum_{p=1}^{P} \sum_{i=1}^{L} \sum_{j=1}^{C} |C_1 - C_2| \times 100\% \tag{6}$$

$$NPCR = \frac{1}{L \times C \times P} \times \sum_{p=1}^{P} \sum_{i=1}^{L} \sum_{j=1}^{C} D(i, j, p) \times 100\% \tag{7}$$

In Eqs. (6) & (7), i, j and p are the row, column, and plane indexes of the image, respectively. While L, C and P are the length, width, and plane sizes of the image. D(i,j,p) = 0 when it is the same value in C_1 and C_2 while it is 1 when it is different. Table 1 presents the results of the plaintext sensitivity attacks of the proposed cryptosystem for the tested images, where the optimal value for UACI is 33.46% and for NPCR is 99.61% which are given in [36, 68].

Two plain images are selected to be encrypted using the same secret key. While they have a difference in one bit in the first block. Most probably, the researchers chose the first bit in

Table 1 Plaintext sensitivity tests for the proposed cryptosystem

Test name	Image name		Masuda	Farajallah	Qumsieh
Plaintext Sensitivity Attack	Lena 256	NPCR	99.614939	99.381388	99.275431
		UACI	33.456859	33.411513	33.386265
		HD	0.499860	0.499240	0.498203
	Lena 512	NPCR	99.609308	99.543568	99.513695
		UACI	33.448059	33.481259	33.431584
		HD	0.499962	0.499812	0.499354
	Lena 1024	NPCR	99.619961	99.594720	99.494553
		UACI	33.510279	33.454623	33.353363
		HD	0.499922	0.500345	0.499837
	Baboon 512	NPCR	99.608044	99.555897	99.556959
		UACI	33.457006	33.457980	33.436678
		HD	0.499965	0.500007	0.499669
	Boat 512	NPCR	99.611649	99.549033	99.551606
		UACI	33.465358	33.443964	33.456685
		HD	0.500025	0.499524	0.499530

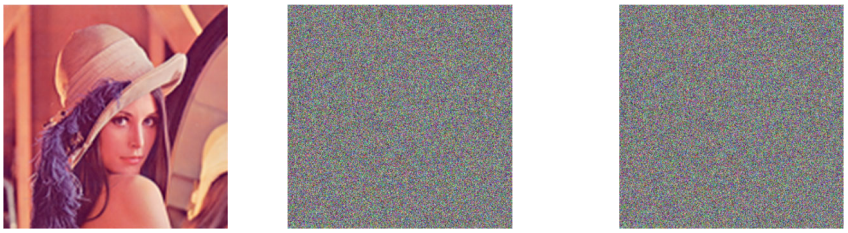
the image to be the different one. For more fair results, another scenario is introduced: the chosen bits will be located in the beginning, in the middle, and at the end of the first block so as to get closer results to the real application.

4.2.2 Key sensitivity attack

As well as the changes of the input, any slight change in the secret key will produce a completely different ciphered image [45], in other words, this means that any cryptosystem has to resist this attack. However, changing one bit in the key during decryption on the ciphered image will completely destroy the decryption process; the whole encryption process will fail.

Figure 5 shows the decryption process of the ciphered Lena image using the same key, but with one bit change in that key at decryption process. This confirms visually that the proposed algorithm resists the sensitivity attacks of the related used keys.

Another testing scenario of the key sensitivity which is similar to the plaintext sensitivity attacks as well: Where, one plaintext P and two secret keys with a difference of one bit.



(a) Plain Lena Image (b) Ciphered Lena Image (c) Decrypted image using incorrect key

Fig. 5 Decryption of lena image using incorrect key

First, P is encrypted using K_1 to obtain C_1. Then the same P is encrypted using K_2 to obtain C_2. Finally, NPCR and UACI are evaluated to calculate the key sensitivity attack of the proposed cryptosystem. As shown in Table 2, the proposed cryptosystem results indicate that the proposed cryptosystem is very sensitive to a one-bit change in the secret key.

5 Statistical analysis

Statistical analysis is used to measure the random behavior of any cryptosystem. In this section, the common statistical tools are used to validate the proposed algorithm.

5.1 Histogram analysis

An image histogram is a graphical demonstration that shows a visual impression of the circulation of pixels through scheming the number of pixels at each grayscale level. This graph shows the number of pixels in an image at each different intensity value.

For encrypted images, the histogram should be uniformly distributed to be strong against the statistical attacks, where cryptnalysis can benefit from the most used bit in the image and its position to reveal some information about the key [34].

The chi-square test's result ensures whether the ciphered image pixels are uniformly distributed or not, as shown in (8) :

$$\chi^2_{exp} = \sum_{i=0}^{Q-1} \frac{(o_i - e_i)}{e_i} \tag{8}$$

where Q is the number of levels (in the proposed model is 256), o_i is the observed occurrence frequencies for each level in the ciphered image and e_i is the expected one from the uniform distribution. In a secure cryptosystem, the experimental chi-square value have to

Table 2 Key sensitivity tests for the proposed cryptosystem

Test name	Image name		Masuda	Farajallah	Qumsieh
Key Sensitivity Attack	Lena 256	NPCR	99.613413	99.609350	99.608515
		UACI	33.462236	33.467554	33.449413
		HD	0.499990	0.499969	0.499957
	Lena 512	NPCR	99.607698	99.610329	99.611708
		UACI	33.460583	33.466205	33.456402
		HD	0.500048	0.500037	0.500021
	Lena 1024	NPCR	99.607817	99.604034	99.604988
		UACI	33.479417	33.450483	33.408832
		HD	0.499907	0.499670	0.499882
	Baboon 512	NPCR	99.606837	99.608943	99.610943
		UACI	33.457946	33.461276	33.462904
		HD	0.499954	0.499968	0.499973
	Boat 512	NPCR	99.608734	99.608728	99.606537
		UACI	33.462312	33.464436	33.463292
		HD	0.499945	0.500036	0.499959

be less than the theoretical chi-square value, which is 293 in case of $\alpha = 0.05$ which is the level of significance and Q = 256, $\chi^2_{exp} < \chi^2_{th}(255, 0.05) = 293$.

More information on setting up the used parameter of the chi-square test can be found on the data analysis book [30].

The results in Fig. 6, show that the tested histograms are uniform and do not reveal any useful information for the statistical analysis.

5.2 Correlation analysis

Two neighboring pixels in a plain image are intensively corresponded in an extreme estimation of relationship coefficient of 1 and the base is 0 considered as the property of an image. On the other hand, the pixels in the encrypted image should have as low redundancy and correlation values as possible (closer to zero), even though the adjacent pixels in the plain images are very redundant and correlated [9].

To define the correlation in the encrypted images [42], the correlation coefficient (r_{xy}) between two horizontally, vertically and diagonally neighboring pixels is calculated for 10000 randomly pairs (N) using the (9)

$$r_{x,y} = \frac{cov(x, y)}{\sqrt{D(x)}\sqrt{D(y)}} \tag{9}$$

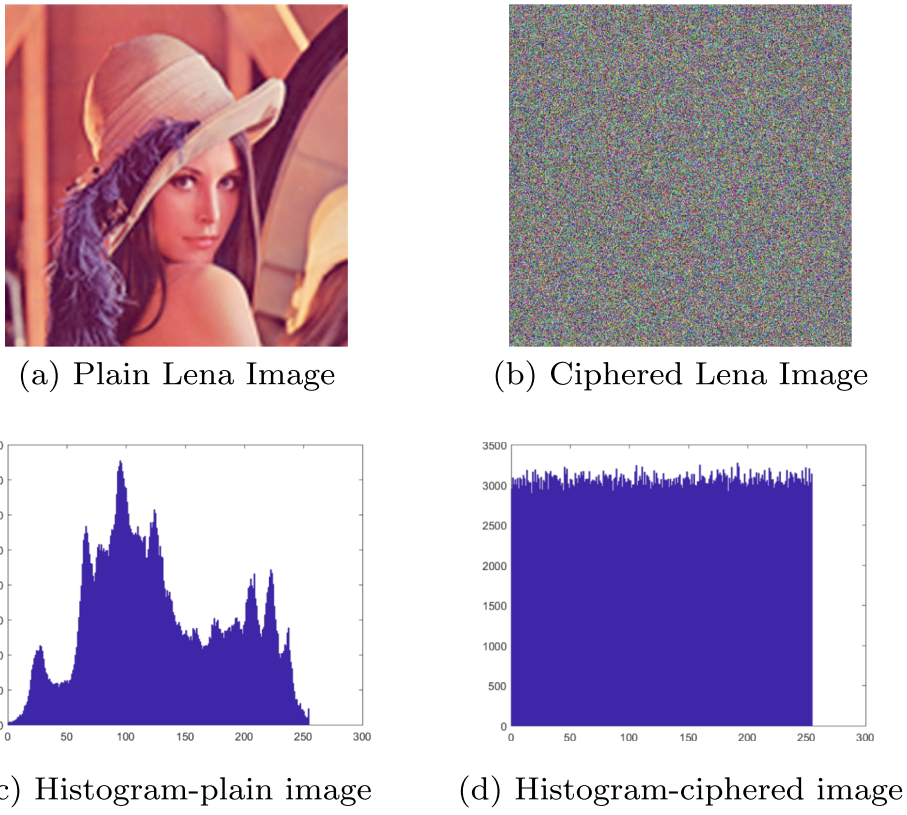


Fig. 6 Lena image 512 plain and ciphered with their Histogram

Table 3 Correlation analysis of the ciphered images

Test name	Image name		Masuda	Farajallah	Qumsieh
Correlation Analysis	Lena 256	Horizontal	0.001830	0.004250	0.009787
		Vertical	0.272201	0.342148	0.333790
		Diagonal	0.003502	0.005918	0.002495
	Lena 512	Horizontal	0.001000	0.015139	0.011517
		Vertical	0.054024	0.090599	0.105004
		Diagonal	0.004644	0.007350	0.013922
	Lena 1024	Horizontal	0.016281	0.002321	0.018429
		Vertical	0.014768	0.025720	0.035597
		Diagonal	0.012571	0.038604	0.004533
	Baboon 512	Horizontal	0.012609	0.000482	0.007449
		Vertical	0.041996	0.108608	0.101798
		Diagonal	0.007462	0.014617	0.000394
	Boat 512	Horizontal	0.014435	0.008261	0.000345
		Vertical	0.048885	0.102851	0.124831
		Diagonal	0.004244	0.007714	0.026092

where $cov(x, y) = \frac{1}{N}\sum_{i=1}^{N}([x_i - E(x)]\,[y_i - E(y)])$, $D(x) = \frac{1}{N}\sum_{i=1}^{N}(x - i - E(x))^2$, $E(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i)$ and x,y are the pixel values of the two adjacent pixels in the tested image.

Table 3 & Fig. 7 show the correlation results for the Lena image and its corresponding cipher image, which is encrypted by the proposed cryptosystem.

5.3 Information entropy

In any image, the values of the pixels are ranging from 0 up to 255. To have a robust algorithm for encrypting, the occurrence probability of any pixel should be almost the same. Thus, the entropy information, which is calculated using (10), will evaluate the random behavior of the encrypted message.

$$H(C) = \sum_{i=0}^{Q-1} Pro(c_i) \times \log_2 \frac{1}{Pro(c_i)} \tag{10}$$

where H(C) is the entropy of the ciphered image C, Pro(c_i) is the occurrence number of each level (i = 0, 1, 2 ... 255). In case of equal probability levels (Pro(c_i) = 2^{-8}), the information entropy is maximal, $H(C) = \sum_{i=0}^{256-1} 2^{-8} \times \log_2(256) = 8$ according to the above (10). Lena image statistics in the proposed cryptosystem, entropy of encrypted image using the proposed algorithm is 7.9996, which is very adjacent to the theoretical value of 8. This shows that the algorithm is secure against entropy attack.

5.4 Encryption quality

In cryptosystems, that encrypts images, pixels values as compared to the value of the same pixel before encryption, where those changes may be irregular [2]. Therefore, this

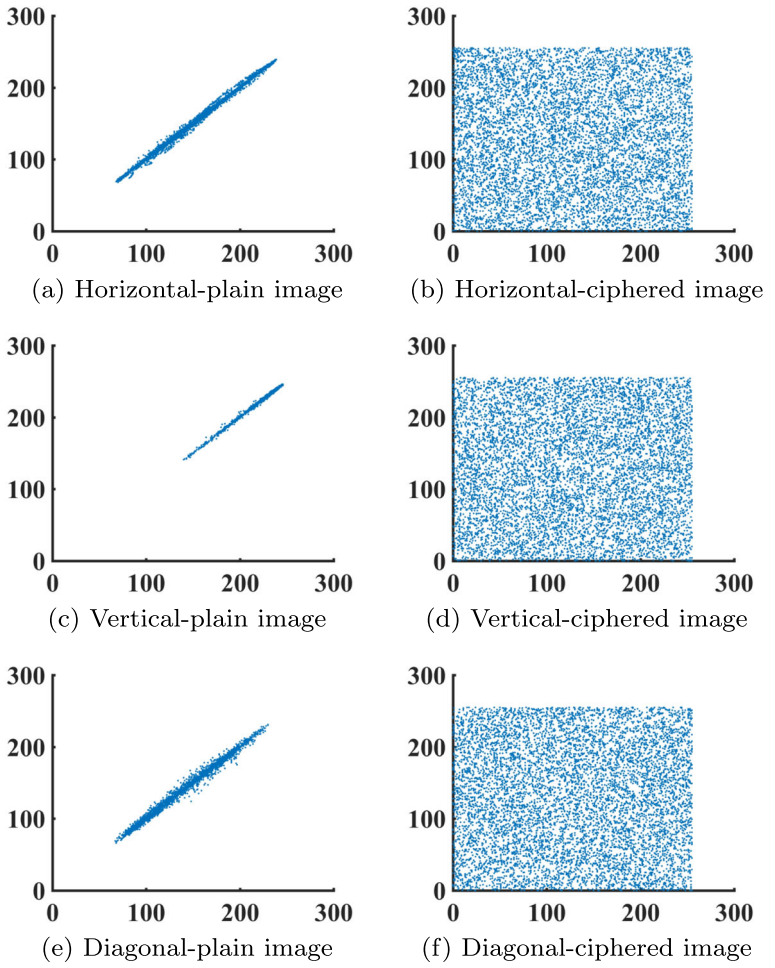


Fig. 7 Correlation analysis of the plain and ciphered Lena image 512

means that the higher the change in the pixels values, the more effective will be the image encryption and the quality of the encryption.

Thus, the encryption quality can be defined as the total changes in pixels values between the original image and the encrypted image and the measure for the encryption quality can be the deviation between the original and encrypted image:

$$EQ = \frac{\sum_{i=1}^{N}(|o_i(P) - o_i(C)|)}{256} \tag{11}$$

where o_i(C) and o_i(P) are the observed occurrences for the byte level i in the ciphered image C and in the plain image P respectively. As a result, the larger the value of EQ, the higher the level of security of the cryptosystem.

For the need of comparison, it is necessary to estimate the optimal value of EQ. The maximal value of EQ denoted as $EQ_{\max}$ [13], $EQ_{\max} = \frac{510 \times L \times C}{256^2}$ where L and C are the line and the column of the gray image/frame, and depending on that the ideal encryption

Table 4 Encryption quality analysis

Test name	Image name	Masuda	Farajallah	Qumsieh
Encryption Quality	Lena 256	286	288	504
	Lena 512	1170	1178	2023
	Lena 1024	4597	4631	8060
	Baboon 512	1373	1381	2036
	Boat 512	1348	1355	2024

quality is 2040. Regarding the Table 4 and Fig. 8, the proposed cryptosystem has a better EQ than the algorithms proposed by [13, 37].

5.5 Complexity analysis

Calculating the complexity of the algorithm used in the cryptosystem is an important factor that determines the time of performance. On the other hand, the performance can be determined by the running speed of the algorithm or the Encryption Throughput (ET), and the number of cycles needed to encrypt one byte, which is the CPU speed in Hertz divided by the ET in bytes [13].

$$ET = \frac{Image_{size}(Byte)}{Encryption_{time}(second)} \tag{12}$$

$$Number\ of\ cycles\ per\ byte = \frac{CPUSpeed_{Herts}}{ET_{Byte}} \tag{13}$$

The results for the encryption and decryption processes of the proposed cryptosystem are carried out using the Code::Blocks compiler of C programming on a laptop with 2.70 GHz

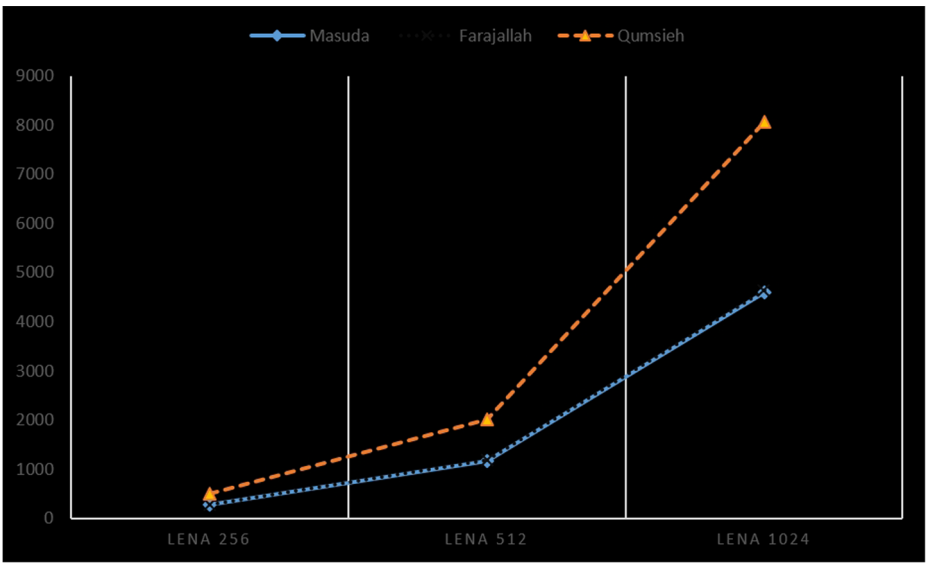


Fig. 8 Encryption quality analysis

Table 5 Encryption time of different algorithms in millisecond

	Lena 256	Lena 512	Lena 1024
Proposed (Qumsieh)	4.60	18.06	54.35
Zhang 1 [72]	7.5	30	120
Zhang 2 [72]	7.5	30	120
Wang [64]	7.79	31.16	124.64
Akhshani [3]	14.4	57.6	230.4
Wong [67]	15.59	62.37	249.48
Kanso [28]	97.15	388	1554
Pareek [47]	160	920	5650
Farajallah [15]	6	24	96
Li [31]	1270	5070	20560
Xu [69]	123	450	–

processor Intel $Core^{TM}$ i7-7500U CPU, 8GB RAM, and Windows 10, 64-bit operation system. Lena image colored with 3 different sizes ((256 × 256 × 3 bytes), (512 × 512 × 3 byte) and(1024 × 1024 × 3 byte)), Baboon and Boat images with the size (512 × 512 × 3 byte) are the image under test. Later, the results were tested again using MATLAB R2017a.

Table 5 presents the running speed of the algorithm (encryption time) in milliseconds, compared with the fastest chaos-based cryptosystems.

To calculate the time performance, the average execution time for the test image after encrypting them using 1000 different secret keys is calculated. Table 6 presents the running speed of the algorithm (throughput) in megabyte per second (MBps) and the number of cycles required to encrypt or decrypt one byte. The results are compared to the fastest chaos-based cryptosystems in the literature. Through those calculations, the number of encryption rounds is identified by the required security level.

Table 6 Encryption throughput and the number of cycles for each encrypted byte - Lena image 512

	ET in MBps	Number of cycles per byte
Proposed (Qumsieh)	41.52	62
Zhang 1 [72]	25	122.07
Zhang 2 [72]	25	122.07
Wang [64]	24.06	122.85
Akhshani [3]	13.02	194.83
Wong [67]	12.03	245.7
Kanso [28]	1.93	1121
Pareek [47]	1.72	554
Farajallah [15]	31.25	94.60
Li [31]	0.148	94.60
Xu [69]	1.53	–

Table 7 Results of the NIST SP 800 - 22 randomness test on encrypted image - Lena image 512

Test name	P value	Binomial Proportion	Results
Frequency test	0.991	10.00	Passed
Block-frequency test	0.739	10.00	Passed
Cumulative-sums test	0.236	10.00	Passed
Runs test	0.350	9.00	Passed
Longest-run test	0.035	10.00	Passed
Rank test	0.122	10.00	Passed
FFT test	0.350	10.00	Passed
Approximate Entropy	0.911	9.00	Passed
Serial test	0.637	10.00	Passed
Linear-complexity	0.213	10.00	Passed

5.6 Randomness tests

To evaluate the proposed algorithm, the well-known NIST test suite are used [54], this test includes 15 test to validate the random behavior of the tested bits. To assess the proposed algorithm, the encrypted images are used as bit-stream for NIST tests to assess the behavior of the encrypted bits.

Based on [23, 54, 60], the observed results in Table 7 confirms that the random behavior of the encrypted version of Lena image 512 with more than 10^6 bits.

Depending on the above results, the proposed algorithm obtained a more robust model with a better security level than the previous models with a faster cryptosystem. The proposed algorithm gave a better key space, a robust model against theoretical attacks, and a more uniformly distributed domain which guaranteed having a faster cryptosystem than the existing ones in the literature, in addition, it preserved the required security level.

6 Conclusion

In recent decades, the most important communication is happening through wireless techniques using the internet to transfer data, and the main concerns remain in the subject of the security. Encryption is a unique way to guarantee the confidentiality of data.

In this paper, the problem of achieving the confidentiality of transmitted images over public channels has been studied, by using chaos-based cryptosystems. The mathematical model of a STM model was improved in this work to be used as the core structure on the proposed cryptosystem that was designed and implemented for real-time applications with a high-security level.

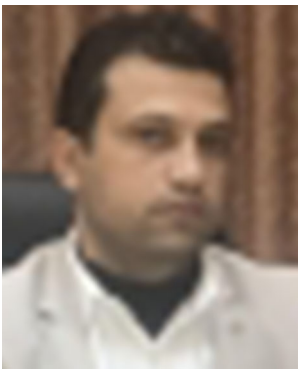
The obtained results confirms the high speed and high security level of the proposed solution regarding statistical tests and some known attacks, however, as a start, any chaos-based encryption algorithm should be evaluated regarding all presented attacks on the classical encryption algorithms in order to be a robust encryption algorithm [49]. The proposed algorithm also can be used in IoT and real-time applications based on the fast encryption process and high security level that has been proved in Section 5. Moreover, it can be modified as future work in order to be used as privacy preservation on the IoT when the key is not change where it is one of the main challenges of the IoT security.

References

1. Ahmad M, Alam MS (2009) A new algorithm of encryption and decryption of images using chaotic mapping. Int J Comput Sci Eng 2(1):46–50
2. Ahmed HE-dH, Kalash HM, Allah OSF (2007) Encryption efficiency analysis and security evaluation of rc6 block cipher for digital images. In: International conference on electrical engineering. IEEE, pp 1–7
3. Akhshani A, Akhavan A, Lim SC, Hassan Z (2012) An image encryption scheme based on quantum logistic map. Commun Nonlinear Sci Numer Simul 17(12):4653–4661
4. Baptista M (1998) Cryptography with chaos. Phys Lett A 240(1-2):50–54
5. Belkhouche F, Qidwai U (2003) Binary image encoding using 1d chaotic maps. In: IEEE Region 5, 2003 annual technical conference. IEEE, pp 39–43
6. Biham E, Shamir A (1991) Differential cryptanalysis of des-like cryptosystems. J Cryptol 4(1): 3–72
7. Brown WS (1971) On euclid's algorithm and the computation of polynomial greatest common divisors. J ACM (JACM) 18(4):478–504
8. Chai X, Chen Y, Broyde L (2017) A novel chaos-based image encryption algorithm using dna sequence operations. Opt Lasers Eng 88:197–213
9. Cohen J, Cohen P, West SG, Aiken LS (2013) Applied multiple regression/correlation analysis for the behavioral sciences. Routledge, Evanston
10. Desmedt YG (2003) Advances in cryptology–CRYPTO'94: 14th Annual International Cryptology Conference, Santa Barbara, California, USA, August 21–25, 1994. Proceedings, vol 839 Springer
11. Ehrsam WF, Meyer CH, Smith JL, Tuchman WL (1978) Message verification and transmission error detection by block chaining. US Patent 4,074,066
12. El Assad S, Noura H (2014) Generator of chaotic sequences and corresponding generating system. US Patent 8,781,116
13. Farajallah M (2015) Chaos-based crypto and joint crypto-compression systems for images and videos. Ph.D. thesis, Universite de Nantes
14. Farajallah M, Assad SE, Deforges O (2018) Cryptanalyzing an image encryption scheme using reverse 2-dimensional chaotic map and dependent diffusion. Multimed Tools Appl 77:28225–28248
15. Farajallah M, El Assad S, Chetto M (2013) 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. IEEE, pp 282–289
16. Farajallah M, Qumsieh R, Isayed S (2016) Selective hybrid chaotic-based cipher for real-time image application. In: The tenth international conference on emerging security information, systems and technologies–SECURWARE 2016
17. Fridrich J (1997) Image encryption based on chaotic maps. In: 1997 IEEE International conference on systems, man, and cybernetics, 1997. Computational cybernetics and simulation, vol 2. IEEE, pp 1105–1110
18. Fridrich J (1997) Secure image ciphering based on chaos. Final report (April, 1997)
19. Fridrich J (1998) Symmetric ciphers based on two-dimensional chaotic maps. Int J Bifurcation Chaos 8(06):1259–1284
20. Gotz M, Kelber K, Schwarz W (1997) Discrete-time chaotic encryption systems. i. statistical design approach. IEEE Trans Circuits Systems I Fund Theory Appl 44(10):963–970
21. Habutsu T, Nishio Y, Sasase I, Mori S (1990) A secret key cryptosystem using a chaotic map. IEICE Trans (1976-1990) 73(7):1041–1044
22. Habutsu T, Nishio Y, Sasase I, Mori S (1991) A secret key cryptosystem by iterating a chaotic map. In: Eurocrypt, vol 91. Springer, pp 127–136
23. Hamza R, Titouna F (2016) A novel sensitive image encryption algorithm based on the zaslavsky chaotic map. Inform Secur J Global Perspective 25(4-6):162–179
24. Han Z, Feng WX, Hui LZ, Da Hai L, Chou LY (2003) A new image encryption algorithm based on chaos system. In: 2003 IEEE international conference on robotics, intelligent systems and signal processing, 2003. Proceedings, vol 2. IEEE, pp 778–782
25. Hraoui S, Gmira F, Jarar A, Satori K, Saaidi A (2013) Benchmarking aes and chaos based logistic map for image encryption. In: 2013 ACS international conference on computer systems and applications (AICCSA). IEEE, pp 1–4
26. Jakimoski G, Kocarev L (2001) Analysis of some recently proposed chaos-based encryption algorithms. Phys Lett A 291(6):381–384

27. Jessa M (2000) Data encryption algorithms using one-dimensional chaotic maps. In: The 2000 IEEE international symposium on circuits and systems, 2000. Proceedings. ISCAS 2000 Geneva, vol 1. IEEE, pp 711–714
28. Kanso A, Ghebleh M (2012) A novel image encryption algorithm based on a 3d chaotic map. Commun Nonlinear Sci Numer Simul 17(7):2943–2959
29. Kocarev L, Jakimoski G, Stojanovski T, Parlitz U (1998) From chaotic maps to encryption schemes. In: Proceedings of the 1998 IEEE International symposium on circuits and systems, 1998. ISCAS'98, vol 4. IEEE, pp 514–517
30. Lewis-Beck M (1995) Data analysis: an introduction. 103. Sage
31. Li C, Luo G, Li C (2019) An image encryption scheme based on the three-dimensional chaotic logistic map. IJ Netw Secur 21(1):22–29
32. Li S, Li Q, Li W, Mou X, Cai Y (2001) Statistical properties of digital piecewise linear chaotic maps and their roles in cryptography and pseudo-random coding. Lect Notes Comput Sci 2260:205–221
33. Li SJ (2003) Analyses and new designs of digital chaotic ciphers. Ph.D. thesis, Xi'an Jiaotong University
34. Liu Y, Nie L, Liu L, Rosenblum DS (2016) From action to activity: sensor-based activity recognition. Neurocomputing 181:108–115
35. Lorenz EN (1963) Deterministic nonperiodic flow. J Atmos Sci 20(2):130–141
36. Maleki F, Mohades A, Hashemi SM, Shiri ME (2008) An image encryption system by cellular automata with memory. In: Third international conference on availability, reliability and security, 2008. ARES 08. IEEE, pp 1266–1271
37. Masuda N, Aihara K (2002) Cryptosystems with discretized chaotic maps. IEEE Trans Circuits Systems I Fund Theory Appl 49(1):28–40
38. Masuda N, Jakimoski G, Aihara K, Kocarev L (2006) Chaotic block ciphers: from theory to practical algorithms. IEEE Trans Circuits Syst Regul Pap 53(6):1341–1352
39. Matthews R (1989) On the derivation of a chaotic encryption algorithm. Cryptologia 13(1):29–42
40. May RM (1976) Simple mathematical models with very complicated dynamics. Nature 261(5560):459–467
41. Muhammad K, Hamza R, Ahmad J, Lloret J, Wang H, Baik SW (2018) Secure surveillance framework for IoT systems using probabilistic image encryption. IEEE Trans Ind Inf 14(8):3679–3689
42. Munir R (2012) Security analysis of selective image encryption algorithm based on chaos and cbc-like mode. In: 2012 7th international conference on telecommunication systems, services, and applications (TSSA). IEEE, pp 142–146
43. Murillo-Escobar M, Abundiz-Pérez F, Cruz-Hernández C, López-Gutiérrez R (2014) A novel symmetric text encryption algorithm based on logistic map. In: Proceedings of the international conference on communications, signal processing and computers (ICNC 14)
44. Murillo-Escobar M, Cruz-Hernández C, Abundiz-Pérez F, López-Gutiérrez R, Del Campo OA (2015) A rgb image encryption algorithm based on total plain image characteristics and chaos. Signal Process 109:119–131
45. Ohm JR, Sullivan GJ, Schwarz H, Tan TK, Wiegand T (2012) Comparison of the coding efficiency of video coding standards–including high efficiency video coding (hevc). IEEE Trans Circuits Syst Video Technol 22(12):1669–1684
46. Pareek N, Patidar V, Sud K (2003) Discrete chaotic cryptography using external key. Phys Lett A 309(1-2):75–82
47. Pareek N, Patidar V, Sud K (2005) Cryptography using multiple one-dimensional chaotic maps. Commun Nonlinear Sci Numer Simul 10(7):715–723
48. Pareek NK, Patidar V, Sud KK (2006) Image encryption using chaotic logistic map. Image Vis Comput 24(9):926–934
49. Preishuber M, Hütter T, Katzenbeisser S, Uhl A (2018) Depreciating motivation and empirical security analysis of chaos-based image and video encryption. IEEE Trans Inf Forensics Secur 13(9):2137–2150
50. Protopopescu VA, Santoro RT, Tolliver JS (1995) Fast and secure encryption-decryption method based on chaotic dynamics. US Patent 5,479,513
51. Rafik H, Zheng Y, Khan M, Paolo B, Faiza T (2019) A privacy-preserving cryptosystem for IoT e-healthcare. Inform Sci
52. Rössler OE (1976) An equation for continuous chaos. Phys Lett A 57(5):397–398
53. Ruelle D (2006) What is a strange attractor. Notices of the AMS 53(7):764–765
54. Rukhin A, Soto J, Nechvatal J, Smid M, Barker E (2001) A statistical test suite for random and pseudorandom number generators for cryptographic applications. Tech. rep., Booz-Allen and Hamilton Inc Mclean Va
55. Schneier B (1993) Description of a new variable-length key, 64-bit block cipher (blowfish). In: International workshop on fast software encryption. Springer, Berlin, pp 191–204

56. Shannon CE (1949) Communication theory of secrecy systems. Bell Labs Tech J 28(4):656–715
57. Sharkovskiĭ A (1995) Coexistence of cycles of a continuous map of the line into itself. Int J Bifurcation Chaos 5(05):1263–1273
58. Sharma M, Kowar MK (2010) Image encryption techniques using chaotic schemes: a review
59. Shujuna L, Xuanqinb M, Yuanlongc C (2001) Pseudo-random bit generator based on couple chaotic systems and its applications in stream-cipher cryptography. In: International conference on cryptology in India (INDOCRYPT), vol 16, p 20
60. Soto J (1999) Statistical testing of random number generators. In: Proceedings of the 22nd national information systems security conference, vol 10. NIST, Gaithersburg, p 12
61. Srividya G, Nandakumar P (2011) A triple-key chaotic image encryption method. In: 2011 International conference on communications and signal processing (ICCSP). IEEE, pp 266–270
62. Tao S, Ruli W, Yixun Y (1998) Perturbance-based algorithm to expand cycle length of chaotic key stream. Electron Lett 34(9):873–874
63. Volos CK, Andreatos AS (2015) Secure text encryption based on hardware chaotic noise generator. J Appl Math Bioinform 5(3):15
64. Wang Y, Wong KW, Liao X, Chen G (2011) A new chaos-based fast image encryption algorithm. Appl Soft Comput 11(1):514–522
65. Wheeler DD (1989) Problems with chaotic cryptosystems. Cryptologia 13(3):243–250
66. William S (1999) Cryptography and network security: principles and practice. Prentice-Hall, Inc, Englewood Cliffs, pp 23–50
67. Wong KW, Kwok BSH, Law WS (2008) A fast image encryption scheme based on chaotic standard map. Phys Lett A 372(15):2645–2652
68. Wu Y, Noonan JP, Agaian S (2011) Npcr and uaci randomness tests for image encryption. Cyber journals: multidisciplinary journals in science and technology. J Selected Areas Telecommun (JSAT): 31–38
69. Xu Q, Sun K, Cao C, Zhu C (2019) A fast image encryption algorithm based on compressive sensing and hyperchaotic map. Opt Lasers Eng 121:203–214
70. Yano K, Tanaka K (2002) Image encryption scheme based on a truncated baker transformation. IEICE Trans Fundam Electron Commun Comput Sci 85(9):2025–2035
71. Zaikin A, Zhabotinsky A (1970) Concentration wave propagation in two-dimensional liquid-phase self-oscillating system. Nature 225(5232):535–537
72. Zhang W, Wong K-w, Yu H, Zhu Z-l (2013) An image encryption scheme using reverse 2-dimensional chaotic map and dependent diffusion. Commun Nonlinear Sci Numer Simul 18(8):2066–2080



Mousa Farajallah received his B.Eng. in Computer Systems Engineering from Palestine Polytechnic University (PPU) in 2006 with high honor and distinguishes (highest rating in PPU system). His master of Electronics and Computer Engineering from AL-Quds university in Jerusalem with Excellent rating (highest rating in AL-Quds University system) in 2010. He studied cryptography course in Saarland University at Germany as Pre-PhD course for cryptography filed in 2012. He received Ph.D. degree in Computer Engineering from NANTES University and INSA Rennes, France in 2015 with exceptional (highest rating in France system). Farajallah Ph.D. thesis deal with crypto-compression solutions of High- Efficiency Video Coding (HEVC) and crypto solutions for real-time applications. Currently, Farajallah is the head of Computer Engineering and Security department at PPU. Farajallah research interests includes: Cryptography, Cryptanalysis, and Crypto-Compression solutions. Farajallah has served more than 8 master students and 30 graduation projects. Farajallah is an active member and reviewer of many high ranked journals, international conferences and workshops and actually he is the president of academic cooperative association in Palestine.

Affiliations

Rawan Qumsieh[1] · Mousa Farajallah[2] · Rushdi Hamamreh[3]

Rawan Qumsieh
rawan.iq@gmail.com

Rushdi Hamamreh
rushdi@staff.alquds.edu

1 Palestine Polytechnic University, Hebron, Palestine

2 Computer Engineering and Security Department, Palestine Polytechnic University, Hebron, Palestine

3 Computer Engineering Department at Al-Quds University, East Jerusalem, Palestine