A New Image Encryption Scheme Using Dual Chaotic Map Synchronization

Obaida Al-Hazaimeh[1], Mohammad Al-Jamal[2], Mohammed Bawaneh[1], Nouh Alhindawi[3], and Bara'a Hamdoni[2]

[1]Department of Computer Science and Information Technology, Al- Balqa Applied University, Jordan
[2]Department of Mathematics, Yarmouk University, Jordan
[3]Faculty of Sciences and Information Technology, Jadara University, Jordan

Abstract: *Chaotic systems behavior attracts many researchers in the field of image encryption. The major advantage of using chaos as the basis for developing a crypto-system is due to its sensitivity to initial conditions and parameter tunning as well as the random-like behavior which resembles the main ingredients of a good cipher namely the confusion and diffusion properties. In this article, we present a new scheme based on the synchronization of dual chaotic systems namely Lorenz and Chen chaotic systems and prove that those chaotic maps can be completely synchronized with other under suitable conditions and specific parameters that make a new addition to the chaotic based encryption systems. This addition provides a master-slave configuration that is utilized to construct the proposed dual synchronized chaos-based cipher scheme. The common security analyses are performed to validate the effectiveness of the proposed scheme. Based on all experiments and analyses, we can conclude that this scheme is secure, efficient, robust, reliable, and can be directly applied successfully for many practical security applications in insecure network channels such as the Internet.*

Keywords: *Chaos, lorenz systems, chen systems, synchronization, cryptography.*

Received April 7, 2020; accepted August 26, 2020
https://doi.org/10.34028/iajit/18/1/11

1. Introduction

Chaos theory has grown significantly over the past few years due to its vast number of applications in different disciplines of information security, physics, engineering, biology, and economy, etc., [23, 24]. However, chaos-related issues have received the attention of both information security professionals and researchers since the 1990s when they started to realize that there is a close relationship between chaos theory and cryptography [16]. Chaos theory is the study that mostly focuses on dynamical systems that are highly sensitive to initial conditions and exhibit chaotic behavior (i.e., random) [15]. Such behavior can arise from complex systems such as the Lorenz system or, very simple non-linear systems such as the Logistic map.

Cryptography can be defined in general as a method used for protecting data (i.e., stored and transmitted) in a form that can only be comprehended by the intended people. In other words, it is the technique of hiding the characteristics of the original data. From the perspective of information security and cryptography, randomness, generated from entirely deterministic systems, is a very appealing property [3]. Many properties of the traditional cryptographic scheme have their corresponding counterparts in chaotic systems such as unpredictability, sensitivity to initial conditions and parameters, diffusion, and confusion. These properties can be utilized with some conventional cryptographic properties of the good cipher (i.e., secure) to resist the statistical analysis attacks [5]. Therefore, these correlations between conventional cryptographic and chaotic systems make them more appealing to work together.

Chaos related issues (i.e., random behavior, sensitivity, diffusion, and confusion) have long received the attention of the information security professionals for developing a crypto-system [8].

Many recent studies have focused on the chaotic cryptography. Al-hazaimeh *et al*. [4] utilized the Lorenz chaotic map to propose a new image encryption algorithm. Sun *et al*. [22] focused on spatial chaos maps to propose a novel image encryption scheme. Al-hazaimeh *et al*. [2] used a 1-D Logistic map to propose a novel image encryption scheme. Guan *et al*. [13] used 1-D Triangular Chaotic Map (i.e., TCM) with a full intensive chaotic population to propose a new scheme. In general, the main idea of chaotic image encryption is to shuffle the positions of the pixels of the plain-image in the spatial domain, then change the pixel values by bitwise XORing with a sequence of a chaotic system. Some of the system parameters and initial conditions are used in the encryption and decryption processes as a secret key [15]. Chaos-based crypto-systems can be divided into two categories i.e., chaos synchronization (i.e., analog form) and independent of chaos synchronization (i.e., digital form) [18].

In recent years, the term synchronization of chaos has emerged. It refers to the tendency of two or many chaotic systems (i.e., equivalent or, non-equivalent) to have the same dynamical behavior [7, 26, 27]. In the field of cryptography and information security, this concept is very attractive since the information is encrypted in the sender side using one chaotic system and then decrypted at the receiver side using the other chaotic system [20]. Since in this case two chaotic systems are involved in such cipher, this in turn enhances and adds much more security features (i.e., secure and robust) to the traditional chaos-based ciphers.

In this article, we devise a new crypto-system based on the chaos synchronization phenomenon in two non-identical chaotic maps to make a new addition to the chaotic based encryption. This addition, provide amaster/slave configuration systems are then utilized to construct a modified chaos-based cipher (i.e., proposed scheme). In particular, we prove that two non-identical chaotic maps such as Lorenz and Chen systems can be completely synchronized under suitable conditions.

This article is organized into four sections including the introduction as follows: the details of the proposed encryption scheme are described in section 2, the experimental results and discussions (i.e., security analyses) are discussed in section 3. The last section i.e., section 4 concludes the present study.

2. Proposed Scheme

In this article, a new chaos-based crypto-system is proposed using the synchronization of the Lorenz and Chen systems. To make it clear, we'll encrypt the plain image using the Lorenz system and decrypt the ciphered image using the Chen system. Several tests are conducted to evaluate and demonstrate the feasibility of the crypto-system. Below, we will prove that the Lorenz and Chen systems can be completely synchronized under suitable conditions and parameters. Then later, we'll discuss in more detail the implementation of the encryption and decryption phases.

2.1. Lorenz Chaotic System

In 1960, Edward N. Lorenz defined the Lorenz system as a dynamical system given by the non-linear differential equations:

$$\begin{aligned} \dot{x} &= a(y-x), \\ \dot{y} &= (\sigma - z)x - y, \\ \dot{z} &= xy - bz. \end{aligned} \tag{1}$$

The system control parameters are a, σ, and b, and the system state variables are x, y, and z. The dynamical system (i.e., Equation (1)) is known to be chaotic when α=10, σ=28, and b=8/3. A chaotic attractor (resembling a butterfly) of the Lorenz system for these value of control parameters are shown in Figure 1. Chaos can be recognized for many dynamical systems by having positive Lyapunov Exponents [12]. In particular, the Lorenz system has positive Lyapunov Exponents for all values of σ in the range [28, 90] (for full details we refer to [4]).

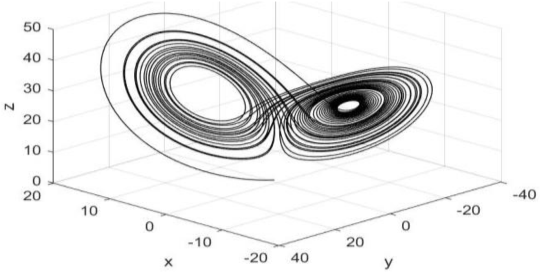


Figure 1. Lorenz system attractor.

2.2. Synchronization via an Active Control Method

From its definition, chaotic systems defy synchronization: that is, synchronization between two chaotic systems seems to be impossible because of the chaotic system signals do not synchronize with any other system. But, the two chaotic systems can synchronize if they exchange information (i.e., establishment) in just the right way [19]. The complete synchronization is the most well-known type of synchronization, in which the interaction between two chaotic systems (whether they are identical or not) leads to a perfect coincidence of their chaotic trajectories, that is: $x_1(t) = x_2(t)$ as $t \to \infty$.

The coupled chaotic systems signals are x_1 and x_2, and t is time [25]. To make it clear, suppose we have two chaotic dynamical systems as

$$\begin{aligned} \dot{x} &= A_1 x + f_1(x), \\ \dot{y} &= A_2 y + f_2(y), \end{aligned}$$

Where A_1x and A_2y are the linear terms, whereas $f_1(x)$ and $f_2(x)$ represent the non-linear parts of the dynamical systems. In the sequel, the drive (i.e., master) will be the first system and there sponse (i.e., slave) will be the second system. The aim is then to make the trajectories of these dynamical systems identical when the time $t \to \infty$. To this end, we add a control function $u(t)$ to the response system, so that $\dot{y} = A_2 y + f_2(y) + u(t)$ Now, the error dynamics is governed by the equation: $e(t)$=$y(t)$–$x(t)$.

Then simple calculations reveal that: $\dot{e} = A_2 e + \mathrm{u} + f$, Where, f=$f_2(y)$–$f_1(x)$+(A_2–A_1)x.

The active control method [14, 6] suggests to choose the controller u so that it eliminates the non-linear term f. To this end, we let u=v–f, where the new control function is$v$. Then it follows that: $\dot{e}$=(A_2e+v).

Now, choose the new controller v as a linear function of the error, say v=Ae. Then, $\dot{e}$=(A_2–A).

If the matrix A is chosen so that the matrix (A_2+A) has negative eigenvalues, then the error$e \to 0$as$t \to \infty$, and hence synchronization is achieved.

2.3. Synchronization

In this section, we construct synchronization between two non-identical chaotic systems. The first is the Lorenz system given by:

$$\begin{aligned} \dot{x_1} &= a(y_1 - x_1), \\ \dot{y_1} &= \sigma x_1 - y_1 - x_1 z_1, \\ \dot{z_1} &= -b z_1 + x_1 y_{1,} \end{aligned} \tag{2}$$

The second chaotic system is the Chen system given by the equations:

$$\begin{aligned} \dot{x_2} &= \alpha(y_2 - x_2), \\ \dot{y_2} &= (\beta - \alpha)x_2 + \beta y_2 - x_2 z_2, \\ \dot{z_2} &= -\gamma z_2 + x_2 y_{2,} \end{aligned} \tag{3}$$

The state variables are x_1=(x_1, y_1, z_1) and x_2=(x_2, y_2, z_2), and the real positive parameters are a, σ, b, a, β, and y. The Lorenz system becomes chaotic when a=10, σ=28, and b=8/3, while the Chen system becomes chaotic when a=35, β=28, and y=3.

To observe the synchronization behavior, we assume that the Lorenz system derives the Chen system. Therefore, the derive system (i.e., master) is given by Equation (2). On the other hand, the response (i.e., slave) is obtained by adding the controller function u_1=(u_1,u_2,u_3) to Chen's system Equation (3). Thus, the response system (i.e., synchronization behavior) is defined by the system of equations:

$$\begin{aligned} \dot{x_2} &= a(y_2 - x_2) + u_1, \\ \dot{y_2} &= (\beta - \alpha)x_2 + \beta y_2 - x_2 z_2 + \ u_2, \\ \dot{z_2} &= -y z_2 + \ \ x_2 y_2 + u_3. \end{aligned} \tag{4}$$

The synchronization error function e=[e_1,e_2,e_3]^T is defined by:

$$\begin{aligned} e_1 &= x_2 - x_1, \\ e_2 &= y_2 - y_1, \\ e_3 &= z_2 - z_1. \end{aligned} \tag{5}$$

The goal is then to design the controller u(t) such that the synchronization error approaches to zero, that is $\lim_{t\to\infty} \|u(t)\| = 0.$

By subtracting Equations (2) from (4), one obtains the error dynamics given by the system of differential equation:

$$\dot{e} = A_1 e + f + u \tag{6}$$

Where the matrix A_1 and the non-linear term f are is given by:

$$A_1 = \begin{bmatrix} -\alpha & a & 0 \\ \beta & -1 & 0 \\ 0 & 0 & -b \end{bmatrix},$$

$$f = \begin{bmatrix} a(x_2 - y_2) + a(y_2 - x_2) \\ (\beta + 1)y_2 - \ a x_2 - x_2 z_2 + x_1 z_1 \\ x_2 y_2 - \ x_1 y_1 - \ (\gamma - b) z_2 \end{bmatrix}$$

In this article, we adopt the active control strategy to design an appropriate controller u. The first stage is to choose u in such a way it eliminates all non-linear terms in the error dynamics Equation (6). To this end, we define u in terms of a new controller v by setting:

$$u = v - f.$$

Therefore, the error dynamics are given by Equation (6) becomes: $\dot{e} = A_1 e + v.$

The next step is to assume that v is a linear function of the error e, that is, v=Ae for some 3×3 matrix A. Consequently, the error dynamics becomes:

$$\dot{e} = Be, \tag{7}$$

Where

$$B = A_1 + A = \begin{bmatrix} -\alpha + \alpha_{11} & a + \alpha_{12} & \alpha_{13} \\ \beta + \alpha_{21} & -1 + \alpha_{22} & \alpha_{23} \\ \alpha_{31} & \alpha_{32} & -b + \alpha_{33} \end{bmatrix}$$

In this article, we need the following definition and lemma to determine the matrix A.

- *Definition* 1: The autonomous system $\dot{x} = Ax$, $x(0) = x_0$, is called *asymptotically stable* if and only if $\lim_{t\to\infty} \|x(t)\| = 0.$

Let spec(A) denote the set of all eigenvalues of A and Re(λ_{i}) denote the realpart of eigenvalueλ_i.

- *Lemma* 1: The autonomous system $\dot{x} = Ax$, $x(0) = x_0$, is asymptotically stable if and only if $\mathrm{Re}(\lambda) < 0$ for all$\lambda \in \mathrm{spec}(A)$.

From Lemma 1, to force the synchronization error to converge to zero, we can choose the matrix A so that $\mathrm{Re}(\lambda) < 0$, for all $\lambda \in \mathrm{spec}(B)$. For example, by choosing a_{11}=a_1–1, a_{12}=–a, a_{21}= –β,a_{33}=b–1,a_{22}=a_{13}=a_{23}=a_{32}=0

We have,

$$A = \begin{bmatrix} \alpha - 1 & a & 0 \\ -\beta & 0 & 0 \\ 0 & 0 & b - 1 \end{bmatrix}, B = \begin{bmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{bmatrix}$$

Therefore, in this case, we have $\mathrm{Re}(\lambda) = -1 < 0$ for all $\lambda \in \mathrm{spec}(B)$, and so theerror system (Equation7) is asymptotically stable:$\|u(t)\|$ → 0, as t → ∞, and hence, the synchronization is achieved. With this matrix$A$, we see that:

$$v = Ae = \begin{bmatrix} (\alpha - 1)e_1 - \alpha e_1 \\ -\beta e_1 \\ (b - 1)e_3 \end{bmatrix}.$$

Substituting in the equation u=v–f, we get after simple simplifications:

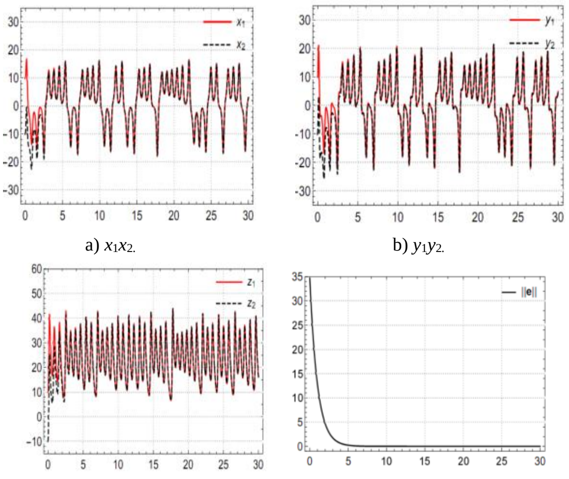
$$u = \begin{bmatrix} (\alpha - 1)x_2 - \ (\alpha - 1)x_1 - \alpha y_2 + \alpha y_1 \\ (\alpha - \beta)x_2 + \ \beta x_1 - (\beta + 1)y_2 + x_2 z_2 - x_1 z_1 \\ (\gamma - 1)z_2 - (b - 1)z_1 - x_2 y_2 + x_1 y_1 \end{bmatrix}$$

Therefore, the states of the response system (i.e., slave) are computed (after simplification) as follows:

$$\dot{x_2} = (1 - \alpha)x_1 - x_2 + \ a y_1,$$

$$\dot{y_2} = \alpha x_1 - y_2 - x_1 z_1,$$
$$\dot{z_2} = -z_2 + (1-b)z_1 + x_1 y_1.$$

As a demonstration, the states of the master and slave systems corresponding to the initial states x_1=(0)=(10,10,10),x_2(0)= (–10,–10,–10),and parameters a=10, b=8/3,σ=28,a=35,β=28,y=3 are plotted in Figure 2.



a) x_1x_2.

b) y_1y_2.

c) z_1z_2.

d) $\|e\|$.

Figure 2. Master and slave systems along with synchronization error.

2.4. Secret Keys Generation

The secret keys for the proposed crypto-system will be the Lorenz parameter σ and the synchronization time T. As mentioned before, chaos (sensitivity to initial conditions) can be recognized for many dynamical systems, Lorenz system in particular by having positive Lyapunov Exponents. In this article, the Maximum Lyapunov Exponents (MLE) of the Lorenz system is computed versus values of $\sigma$and plotted in Figure 3.

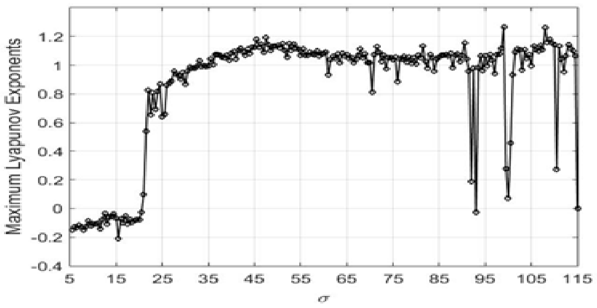


Figure 3. Maximum lyapunov exponents.

For the proposed crypto-system, we shall fix the parameters to a=10,b=8/3,a=35,β=28, and y=3, but we will allow σ to beany number in the interval [28, 90] (in which the master system is chaotic). The encrypted images will be protected against brute-force attacks due to the large keyspace. In cryptography, this will guarantee denser (chaotic) attractors forthe master system, thus trajectories will remain in the same attractor set regardless of any variations in the initial conditions, and hence, this will make it nearly impossible to predict any outcome without the exact knowledge of initial conditions and the iteration counts in the numerical solution.

2.5. Encryption Scheme

Generally, encryption can be defined asa set of processes over the original image to conceal the characteristics and features of the original image. These processes perform several permutations of transformations, transpositions, and substitutions in a specific order [1, 16]. In this article, we use the drive system (i.e., master) in the encryption process and we assume that the synchronization is achieved between the Lorenz system and Chen system at time T as shown in Figure 4. The proposed encryption scheme is based on a set of sequential and parallel steps, described as follows:

Steps of the proposed encryption scheme

1. Re-arrange the pixels of the plain image $I_{m\times n}$ from top to bottom and then left to right to get the set P={p_1,p_2,p_3,...,p_d}, where d=mn, each element in P is the 8–bit representation of the gray value of the corresponding pixel.
2. Simulate the master and slave systems until complete synchronization is observed. Suppose that the synchronization is achieved at t=T.
3. Iterate the master system for $t \geq T$ to generate three chaotic decimal sequences: X={x_1, x_2, x_3,...},Y={y_1, y_2, y_3,...},Z={z_1, z_2, z_3,...}. Obtain new sequence
   $$\text{XY} = \{x_1, y_1, x_2, y_2, x_3, y_3, \ldots\}.$$
4. Then for each element in the sequences XY do the following:
   - Normalize then chop.
   - Extract the mantissa by removing the decimal point.
   - Take the mantissa module 256 to get an integer in the interval [0, 255].
   - Convert it into 8–bit binary representation.

   The resulted sequence will be denoted by S={s_1,s_2,s_3,...}.
5. For each element in the sequence Z do the following:
   - Normalize then chop.
   - Extract the mantissa by removing the decimal point.
   - Take the mantissa module 3 to get an integer in the interval [0, 2].

   The resulted sequence will be denoted by R={r_1,r_2,r_{13},...}.
6. Generate the set Q={q_1, q_2, q_3, . . . , q_d} via the loop: j ← 0; For each i = 1, 2, . . . d :j ← j +r_i + 1; q_i ← s_j .
7. Finally, by the XOR operation the ciphered image C is obtained: $C = P \oplus Q$.

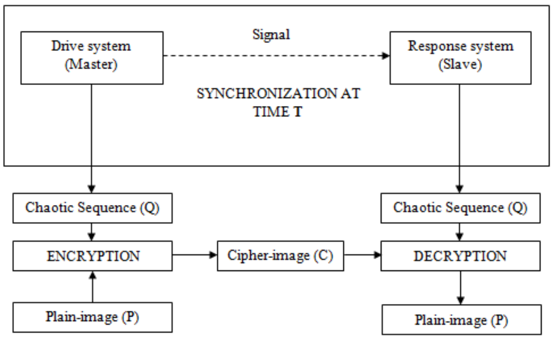


Figure 4. Encryption scheme.

The decryption scheme is almost the same as the encryption scheme (i.e., previous steps) but with reverse order as the diagram in Figure 5.

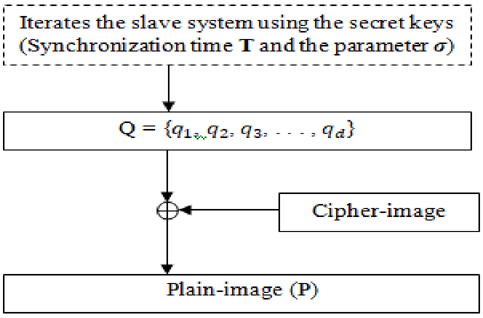
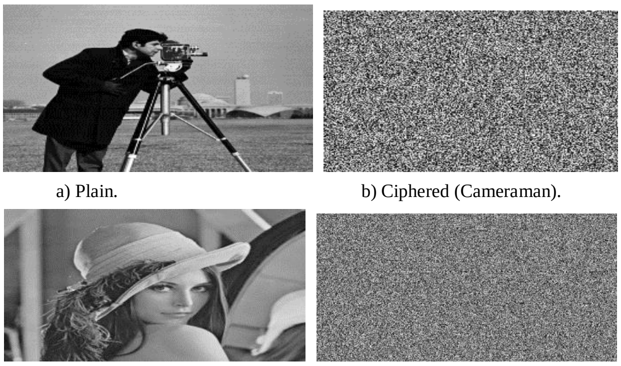

Iterates the slave system using the secret keys
(Synchronization time T and the parameter σ)
$Q = \{q_1, q_2, q_3, ..., q_d\}$
Cipher-image
Plain-image (P)

Figure 5. Decryption scheme.

3. Results and Discussion

To evaluate the security level, some of the experimental results (i.e., simulations) are given in this section. The experiments are performed on the test images which are available in several public domains. The plain images along with their ciphered images by the proposed scheme as presented in Figure 6. We have fixed the secret key to σ=28, in which case the synchronization time is observed when T=40. Below, we have given several security tests such as histogram, key space, information entropy, correlation, key sensitivity, differential attacks, and randomness to assess the security features of the proposed crypto-system [4, 9, 11, 17, 21, 22] as shown in Figure 7 (see Appendix A, for the detail of the security analysis relations).



a) Plain. b) Ciphered (Cameraman).

c) Plain. d) Ciphered (Lena).

Figure 6. Plain and ciphered images.

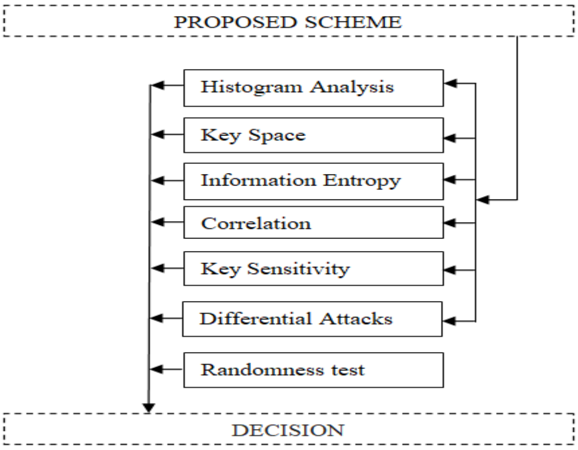
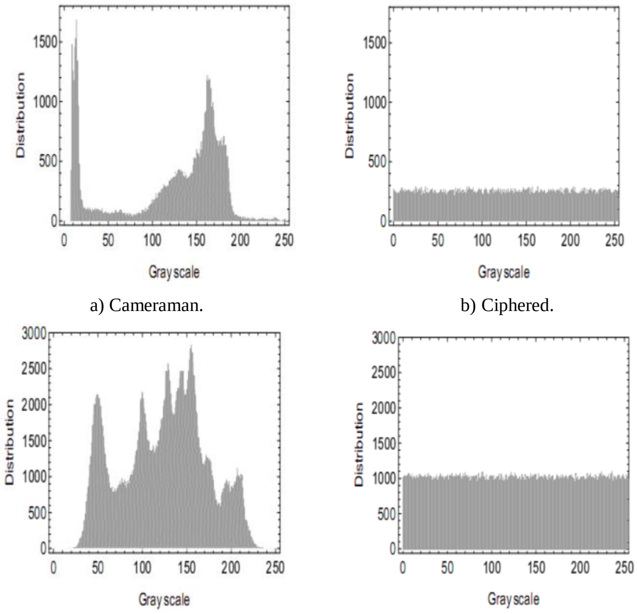


Figure 7. Security analysis structure.

3.1. Histogram Analysis

The histogram distributions for the plain and the corresponding ciphered images by the proposed scheme are displayed in Figure 8. It is clear from Figure 8 the histogram analyses of the ciphered images are significantly different and fairly uniform from those of the plain images.



a) Cameraman. b) Ciphered.

c) Lena. d) Ciphered.

Figure 8. Histograms analysis.

3.2. Key Space

In the proposed scheme, the synchronization time T and the parameter σ of the Lorenz systemare the secret keys. In a double-precision system, the key space size will be 10^{28} which is extremely large that would resist the brute force attacks.

3.3. Information Entropy

The information entropy (i.e., randomness or, disorder measurements) was calculated in this article and listed in Table 1. As can be seen from Table 1, the result shows that the entropy values are very close to 8 [10].

This analysis confirms that the proposed scheme is secure against the entropy attack (i.e., information leakage is negligible).

Table1. Entropy.

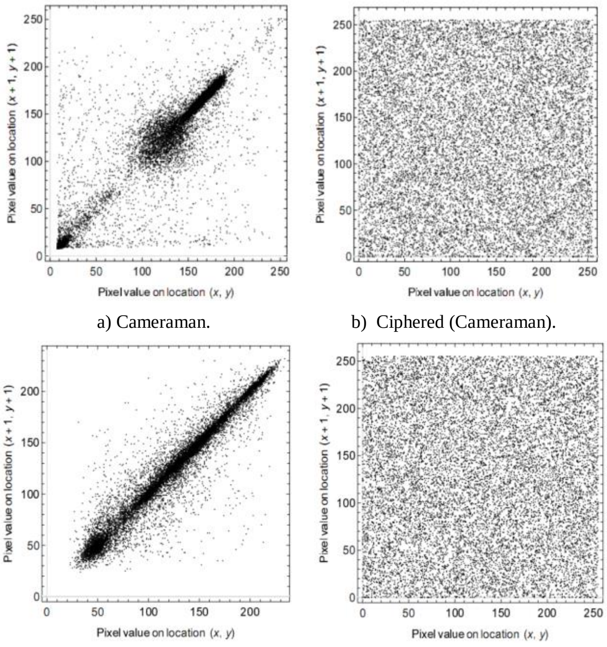
Images	Plain	Ciphered
Cameraman	7.0097	7.9871
Lena	7.4462	7.9994

3.4. Correlation

The statistical analysis has been performed on the proposed scheme by testing the correlation of 15, 000 pairs of two adjacent pixels (i.e., horizontally, vertically, and diagonally) which are selected randomly. The average correlation coefficient values are displayed in Table 2, while Figure 9 shows the correlation distribution of the two adjacent pixels in simulated plain and ciphered images. Overall, the obtained results show that the features of the plain image are concealed successfully by the proposed scheme that would resist the statistical attacks.

Table 2. Correlation.

Images	Plain Horizontal	Plain Vertical	Plain Diagonal	Ciphered Horizontal	Ciphered Vertical	Ciphered Diagonal
Cameraman	0.9334	0.9566	0.9091	0.0083	0.00615	0.0058
Lena	0.9705	0.9856	0.9581	0.0054	0.0059	0.0044



a) Cameraman.

b) Ciphered (Cameraman).

c) Lena.

d) Ciphered (Lena).

Figure 9. Correlations analysis.

3.5. Key Sensitivity and Differential Attacks

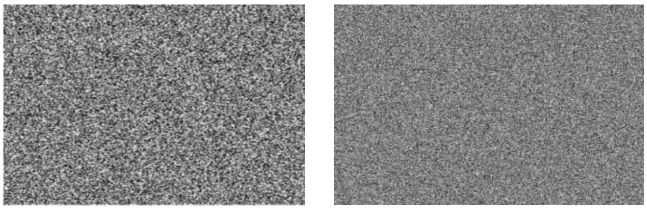
Further, we test the NPCR and UACI to verify the key sensitivity between original images and recovered images. The calculated NPCR and UACI values of the test images due to a slight change in the secret keys are displayed in Tables 3 and 4. The decrypted images corresponding to the incorrect secret key $\sigma = 28.0000000000005$ are depicted in Figure10, while the decrypted images corresponding to the incorrect secret key T=40.0000000000005 are shown in Figure 11.

Table 3. NPCR and UACI values due to a slight change in σ.

Test	Cameraman	Lena
NPCR	0.996078	0.996029
UACI	0.334214	0.335408

Table 4. NPCR and UACI values due to a slight change in T.

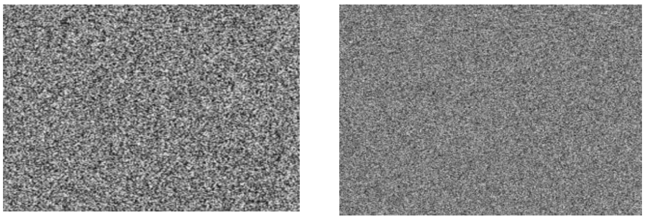
Test	Cameraman	Lena
NPCR	0.995721	0.993706
UACI	0.333044	0.334664



a) Cameraman.

b) Lena.

Figure 10. Decryption using incorrect secret key σ.



a) Cameraman.

b) Lena.

Figure 11. Decryption using incorrect secret key T.

3.6. Randomness Tests

In cryptography, various statistical test suites have been developed such as Crypt-XS, NIST, and Diehard to assess whether the ciphered image behaves like random or not [4]. The obtained results from Diehard and NIST test suites are summarized in Tables 5 and 6. From these results, we see that the ciphered images have passed successfully all the tests, then this means that they exhibit chaotic behavior (i.e., random)and weak correlation of sequence.

Table 5. DIEHARD tests suite.

Test		Average	Behavior
OPSO		0.5003	Random
Runs		0.591687	Random
Ones count	01	0.578156	Random
	02	0.297760	Random
Bit stream		0.52682	Random
Spacing	Birthday	0.517851	Random
OQSO		0.4663	Random
Craps		0.313835	Random
Binary rank	31 × 31	0.927171	Random
	32 × 32	0.356173	Random
Spheres	3DS	0.324662	Random
Distance	Minimum	0.601171	Random
Parking lot		0.725481	Random
Squeeze		0.645418	Random
Overlapping	Sum	0.571485	Random
	Permutation	0.485734	Random
DNA		0.5876	Random

Table 6. NIST test suite.

Test		***P*-value**	**Behavior**
Complexity	Lempel-ziv	0.651440	Random
	Serial	0.483238391	Random
	Linear	0.455452544	Random
Ones	Long runs	0.392153501	Random
Entropy	Approximately	0.577572377	Random
DFT	Spectral	0.5521431	Random
Templates	No overlapping	0.600957	Random
Universal	Q = 1280, K = 141 577, and L = 7	0.382153447	Random
Frequency	Universal	0.354456496	Random
	Block	0.515845856	Random
Runs	M = 10 000	0.495274156	Random
Rank		0.444765232	Random
Sums	Forward	0.39263215	Random
	Reverse	0.398473236	Random
Excursions (Randomly)	X = −4	0.657282	Random
	X = 4	0.49816	Random

4. Conclusions

This article has focused on proposed a new encryption scheme using dual chaotic map synchronization. In particular, we have proved that the two non-identical chaotic maps such as Lorenz and Chen systems can be completely synchronized under suitable conditions which make a new addition to the chaotic based encryption. This addition, provide a master/slave configuration systems are then utilized to construct a proposed chaos-based cipher scheme. To verify the effectiveness of the proposed scheme, the security features are analyzed thoroughly and show that this article made an important contribution by providing a robust and very secure scheme that can be adopted in various security applications.

References

[1] Al-hazaimeh O., "Increase the Security Level for Real-Time Application Using New Key Management Solution," *International Journal of Computer Science Issues*, vol. 9, no. 3, pp. 240-247, 2012.

[2] Al-hazaimeh O., "A Novel Encryption Scheme for Digital Image-Based on one Dimensional Logistic Map," *Computer and Information Science*, vol. 7, no. 4, pp. 64-73, 2014.

[3] Al-hazaimeh O., "A New Dynamic Speech Encryption Algorithm Based on Lorenz Chaotic Map over Internet Protocol," *International Journal of Electrical and Computer Engineering*, vol. 10, no. 5, pp. 4824-4834, 2020.

[4] Al-hazaimeh O., Al-Jamal M., Alhindawi N., and Omari A., "Image Encryption Algorithm Based on Lorenz Chaotic Map with Dynamic Secret Keys," *Neural Computing and Applications*, vol. 13, no. 3, pp. 2395-2405, 2017.

[5] Arthanari S., Mastan M., and Bagank B., "Chaotic Image Encryption using Modular Addition and Combinatorial Techniques," *The International Arab Journal of Information Technology*, vol. 12, no. 2, pp. 110-117, 2015.

[6] Bhalekar S. and Daftardar-Gejji V., "Synchronization of Different Fractional Order Chaotic Systems Using Active Control," *Communications in Nonlinear Science and Numerical Simulation*, vol. 15, no. 11, pp. 3536-3546, 2010.

[7] Boccaletti S., Kurths J., Osipov G., Valladares D., and Zhou C., "The Synchronization of Chaotic Systems," *Physics Reports*, vol. 366, no. 1-2, pp. 1-101, 2002.

[8] Coppersmith D., "The Data Encryption Standard (DES) and its Strength Against Attacks," *IBM journal of Research and Development*, vol. 38, no. 3, pp. 243-250, 1994.

[9] El-Samie A., Ahmed H., Elashry F., Shahieen H., Faragallah S., El-Rabaies M., and Alshebeili A., *Image Encryption: A Communication Perspective*, CRC Press, 2013.

[10] Fraser M., "Information and Entropy in Strange Attractors," *IEEE Transactions on Information Theory*, vol. 35, no. 2, pp. 245-262, 1989.

[11] Fridrich J., "Symmetric Ciphers Based on Two-Dimensional Chaotic Maps," *International Journal of Bifurcation and Chaos*, vol. 8, no. 6, pp. 1259-1284, 1998.

[12] Govorukhin V., "Calculation Lyapunov exponents for ODE," *MATLAB Central File Exchange*, File ID: 4628, 2004.

[13] Guan Z., Huang F., and Guan W., "Chaos-based Image Encryption Algorithm," *Physics Letters A*, vol. 346, no. 1-3, pp. 153-157, 2005.

[14] Ho M. and Hung Y., "Synchronization of Two Different Systems By Using Generalized Active Control," *Physics Letters A*, vol. 301, no. 5-6, pp. 424-428, 2002.

[15] Kocarev L., "Chaos-Based Cryptography: A Brief Overview," *IEEE Circuits and Systems Magazine*, vol. 1, no. 3, pp. 6-21, 2001.

[16] Lü H., Wang S., Li X., Tang G., Kuang J., Ye W., and Hu G., "A New Spatiotemporally Chaotic Cryptosystem and its Security and Performance Analyses," *Chaos: An Interdisciplinary Journal of Nonlinear Science*, vol. 14, no. 3, pp. 617-629, 2004.

[17] Muthukumar P., Balasubramaniam P., and Ratnavelu K., "A Novel Cascade Encryption Algorithm for Digital Images Based on Anti-Synchronized Fractional order Dynamical Systems," *Multimedia Tools and Applications*, vol. 76, no. 22, pp. 23517-23538, 2017.

[18] Parlitz U., Chua O., Kocarev L., Halle K., and Shang A., "Transmission of Digital Signals by Chaotic Synchronization," *International Journal of Bifurcation and Chaos*, vol. 2, no. 4, pp. 973-977, 1992.

[19] Pecora M. and Carroll L., "Synchronization of Chaotic Systems," *Chaos: An Interdisciplinary*

Journal of Nonlinear Science, vol. 25, no. 9, 2015.

[20] Sayed S. and Radwan G., "Generalized Switched Synchronization and Dependent Image Encryption Using Dynamically Rotating Fractional-Order Chaotic Systems," *AEU-International Journal of Electronics and Communications*, vol. 123, no. 1, pp. 153-268, 2020.

[21] Shannon E., "Communication Theory of Secrecy Systems," *Bell System Technical Journal*, vol. 28, no. 4, pp. 656-715, 1949.

[22] Sun F., Liu S., Li Z., and Lü Z., "A Novel Image Encryption Scheme Based on Spatial Chaos Map," *Chaos, Solitons and Fractals*, vol. 38, no. 3, pp. 631-640, 2008.

[23] Tahat N., Tahat A., Abu-Dalu M., Albadarneh B., Abdallah E., and Al-Hazaimeh O., "A new RSA Public Key Encryption Scheme with Chaotic Maps," *International Journal of Electrical and Computer Engineering*, vol. 10, no. 2 , pp. 1430-1437, 2020.

[24] Tél T. and Gruiz M., *Chaotic Dynamics: An Introduction Based on Classical Mechanics*, Cambridge University Pres, 2006.

[25] Volos C., Kyprianidis M., and Stouboulos N., "Image Encryption Process Based on Chaotic Synchronization Phenomena," *Signal Processing*, vol. 93, no. 5, pp. 1328-1340, 2013.

[26] Wang L., Dong T., and Ge M., "Finite-Time Synchronization of Memristor Chaotic Systems and its Application in Image Encryption," *Applied Mathematics and Computation*, vol. 347, pp. 293-305, 2019.

[27] Weng T., Yang H., Gu C., Zhang J., and Small M., "Synchronization of Chaotic Systems And Their Machine-Learning Models," *Physical Review E*, vol. 99, no. 4, pp. 042203, 2019.

Obaida Al-Hazaimeh is an Associate Professor of Computer Science. Now, he is a lecturer at Department of Computer Science and Information Technology. Al-Balqa' Applied University, Jordan. He has received his Ph.D. in Computer Science-Cryptography from Malaysia in 2010.

Mohammad Al-Jamal is an Associate Professor of Mathematics. Now, he is a lecturer at Department of Mathematics, Yarmouk University, Jordan. He has earned his Ph.D. in Mathematics from USA in August 2012.

Mohammed Bawaneh is an Associate Professor of Computer science. Now, he is a lecturer at Department of Computer Science and Information Technology. Al-Balqa' Applied University, Jordan. He has earned his Ph.D. in Computer Information Systems in 2010.

Nouh Alhindawi is an Associate Professor in Computer Science & Software Engineering Departments at Jadara University, Jordan. He has received his Ph.D. in Computer Science-Software Engineering from USA in 2013.

Bara'a Hamdoni received her BSc in Mathematics from Jordan University of Science and Technology in 2012, and MSc in Mathematics with specialization in Image Encryption from Yarmouk University in 2018.

Appendix A. Common equations related to security analysis

- ENTROPY

$$H(s) = \sum_{i=1}^{2N-1} P(s_i) \log_2 \frac{1}{P(s_i)}$$

- CORRELATION:

$$r_{xy} = \frac{\operatorname{cov}(x,y)}{\sqrt{D(x)\sqrt{D(y)}}}$$

$$\operatorname{cov}(x,y) = \frac{1}{N}\sum_{i=1}^{N}\big(x_i - E(x)\big)\big(yi - E(y)\big),$$

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

- DIFFERENTIALS:

$$\text{NPCR} = \frac{1}{W \times H}\left[\sum_{i,j} D(i,j)\right] \times 100\%$$

$$\text{UACI} = \frac{1}{W \times H}\left[\sum_{i,j}\frac{C_1(i,j) - C_2(i,j)}{255}\right] \times 100\%$$