symmetry

MDPI

Article

A New 4D Hyperchaotic System with Dynamics Analysis, Synchronization, and Application to Image Encryption

Tsafack Nestor [1], Akram Belazi [2], Bassem Abd-El-Atty [3], Md Nazish Aslam [4], Christos Volos [5,*], Nkapkop Jean De Dieu [6] and Ahmed A. Abd El-Latif [7,8]

1 Research Unit of Laboratory of Automation and Applied Computer (LAIA), Electrical Engineering Department of IUT-FV, University of Dschang, Bandjoun P.O. Box 134, Cameroon; nestor.tsafack@yahoo.fr
2 Laboratory RISC-ENIT (LR-16-ES07), Tunis El Manar University, Tunis 1002, Tunisia; akram.belazi@enit.utm.tn
3 Department of Computer Science, Faculty of Computers and Information, Luxor University, Luxor 85957, Egypt; bassem.abdelatty@fci.luxor.edu.eg
4 Piro Technologies Pvt. Ltd., New Delhi 110025, India; nazi34u@gmail.com
5 Laboratory of Nonlinear Systems, Circuits and Complexity (LaNSCom), Department of Physics, Aristotle University of Thessaloniki, 54124 Thessaloniki, Greece
6 Department of Electrical Engineering and Industrial Computing, University Institute of Technology, Douala P.O. Box 8698, Cameroon; golby01@yahoo.fr
7 EIAS Data Science Lab, College of Computer and Information Sciences, Prince Sultan University, Riyadh 11586, Saudi Arabia; a.rahiem@gmail.com or aabdellatif@nu.edu.eg
8 Department of Mathematics and Computer Science, Faculty of Science, Menoufia University, Shebin El-Koom P.O. Box 32511, Egypt
* Correspondence: volos@physics.auth.gr

Abstract: In this paper, a new 4D hyperchaotic nonlinear dynamical system with two positive Lyapunov exponents is presented. Exhaustive dynamic analyses of the novel hyperchaotic model using several dynamical studies are described. The dynamics of the system considered are first investigated analytically and numerically to explore phenomena and the selection of hyperchaotic behavior utilized for designing image cryptosystem. Since the proposed hyperchaotic model has rich dynamics, it displays hidden attractors. It emerges from this dynamic the existence of a single unstable equilibrium point giving rise to self-excited attractors, hysteresis phenomenon, and hyperchaotic behavior strongly recommended for securing information by its character. Furthermore, the feasibility and synchronization of the proposed system are also presented by developing, respectively, Raspberry surveys and an adaptive synchronization approach of two identical hyperchaotic systems. By employing the hyperchaotic behavior of the 4D map, an image encryption scheme is proposed as well. It is one round of a pixel-based permutation and a bit-wise diffusion phase. The secret key of the 4D map is derived from the SHA-256 value of the input image. It acts as the signature of the input image. Hence, the secret key exhibits high sensitivity to single-bit alteration in the image, which makes the cryptosystem robust against chosen/known-plaintext attacks. Performance analyses prove that the proposed cryptosystem provides the best in terms of the performance/complexity trade-off, as compared to some recently published algorithms.

Keywords: image cryptosystem; hyperchaotic system; self-excited attractors; adaptive synchronization; hysteresis phenomenon; SHA-256

Citation: Nestor, T.; Belazi, A.; Abd-El-Atty, B.; Aslam, M.N.; Volos, C.; De Dieu, N.J.; Abd El-Latif, A.A. A New 4D Hyperchaotic System with Dynamics Analysis, Synchronization, and Application to Image Encryption. *Symmetry* **2022**, *14*, 424. https://doi.org/10.3390/sym14020424

Academic Editor: Sergio Elaskar

Received: 7 January 2022
Accepted: 2 February 2022
Published: 21 February 2022

1. Introduction

With accelerated cybercrimes due to the rapid growth of the Internet and the latest technologies, multimedia information is increasingly transmitted online. Digital images are widely used daily due to their usefulness. Spying affects a wide range of data, notably passwords, email messages, bank codes, digital images, videos, etc. These attachments generally used daily can enter the individual or public sectors, institutions, or states in

diverse sectors such as the medical, military, industrial, and many others; hence, there is an obligation to preserve and secure the data exchanged. Image encryption is one of the leading solutions. Still, due to the high correlation between the pixels of the image, the high redundancy of the exchanged images, and the particular type of image format, classic text encryption technology such as Advanced Encryption Standard (AES), IDES (International Data Encryption Standard), Data Encryption Standard (DES), and many others prove ineffective for the needs of image encryption [1,2]. Therefore, the development of new secure, robust, and efficient image encryption techniques will always be at the center of trade and communications [3,4]. Chaos-based cryptography is an occasion as a chaotic model has some fundamental features (sensitivity to primary conditions and parameters, randomness, and non-periodicity) for keeping communications secure. Therefore, there is a familiar presence among chaos and cryptography within several studies [5]. Numerous scholars have dedicated themselves to studying chaotic systems for reliable knowledge of these systems to grow nonlinear science [6–18]. As an outcome, chaotic models have developed, following the wanted task. Chaotic models are categorized into two classes depending on the type of equilibrium points: systems with hidden attractors and self-excited attractors. Self-excited attractors are correlated with a saddle or unstable equilibria while hidden attractors are not [19–21]. Other scholars have focused on the nature of nonlinearities such as hyperbolic, quadratic, cubic, and exponential nonlinearity systems [22,23]. Latterly, a class of scholars has focused on the development and study of novel chaotic models without linear features [8,24].

The stochastic properties of chaotic or hyperchaotic systems are generally utilized for securing data [25]. One-dimensional systems, chaotic or hyperchaotic models with multi-dimensions, have been used for designing various cryptosystems [26–28]. Image encryption techniques have vast applications in many areas of everyday life, such as electronic medical records, to name a few. Such medical records are used for diagnosis, transmission, treatment, and sometimes even to reproduce patients' medical history. This should be performed in strict patient privacy. The use of hyperchaotic behavior in image encryption techniques can improve the security of such cryptosystems.

One-dimensional chaotic systems have a simplistic structure and are straightforward to execute. However, they have a small secret keyspace, a low chaotic behavior, a low Lyapunov exponent, and, therefore, a low-security level [29]. Accordingly, improved encryption techniques for one-dimensional chaotic maps have been presented. Thus, Wu and colleagues in their work have improved the existing one-dimensional chaotic behavior and subsequently proposed a new image encryption scheme [30]. As a result, Hua and coworkers proposed combining two chaotic one-dimensional maps in parallel to obtain a new one-dimensional chaotic map for image encryption [31], which broadened the scope of the chaotic mapping of the system. This enlargement method, similarly to many others, improves chaotic characteristics to some extent, but the system parameters remain limited.

As for chaotic or hyperchaotic multidimensional systems, their parameters have more flexibility, their phase space is complex, and their dynamic behavior is difficult to predict. In addition, dynamic systems with better hyperchaotic characteristics have two or more positive Lyapunov exponents, which are better than one-dimensional chaotic maps. Such a multidimensional system can produce several chaotic sequences (keys) at the same time, which can be used in scrambling and broadcasting images, respectively, with high-security [32].

Motivated by limits observed in one-dimensional chaotic models, a new encryption technique based on hyperchaotic behavior in addition to permutation and diffusion operations is presented in this study. It consists of pixel-based permutation and bit-wise diffusion phases under one round. The secret key of the cryptosystem is derived from the input image signature, i.e., its 256-bit long hash value. This dependence improved sensitivity to tiny changes in the original image and the initial keys, limiting the impact of known/chosen plaintext attacks.

Analytical and numerical analyzes reveal the following:

- The dynamic system is considered at a single unstable equilibrium point, with two positive Lyapunov exponents and, therefore, is hyperchaotic;
- The feasibility and synchronization of the model under investigation are, respectively, confirmed and justified.
- The proposed cryptosystem meets the criteria of a robust encryption scheme, including a large keyspace, resistance to statistical, differential, and chosen/known-plaintext attacks.

Furthermore, the proposed cryptosystem possesses a linear running time, indicating its low complexity and fitness for practical use.

The layout of this paper is as follows: Section 2 provides the investigated system. An analytical study of the system consisting of dissipativity, symmetry, fixed points, and stability is presented in Section 3. Section 4 investigates the complete dynamic performance, as well as the numerous phenomena observed and Raspberry studies for the effectiveness of the suggested hyperchaotic system. An adaptive synchronization scheme of two identical systems studied is presented in Section 5. Section 6 describes the proposed encryption image scheme, while Section 7 reports the outcomes of statistical and differential tests. Finally, Section 8 concludes the paper.

2. The Hyperchaotic System

The dynamic system studied in this article is obtained from the oscillator previously presented by Liu et al. [33] by replacing the cubic nonlinearity with a hyperbolic sine nonlinearity. This modification is performed to simplify the practical circuit design, given that the hyperbolic sine nonlinearity is realized by two diodes connected in antiparallel. In contrast, cubic nonlinearity is realized by analog multipliers:

$$\begin{cases} \dot{x}_1 = \beta_1(x_2 + 0.2(x_1 - \varepsilon \sinh(x_1))), \\ \dot{x}_2 = \beta_2 x_1 - x_2 + x_3 + x_4, \\ \dot{x}_3 = -\beta_3 x_2 + x_4, \\ \dot{x}_4 = -\beta_4 x_1, \end{cases} \tag{1}$$

where the state variables are x_1, x_2, x_3, and x_4 and positive parameters are β_1, β_2, β_3, and β_4. The only state variable responsible for the complex behavior is x_1 linked to the hyperbolic nonlinearity.

3. Characteristics of the Hyperchaotic System

3.1. Dissipativity and Symmetry

The condition to investigate the dissipation of (1) is described as in (2):

$$\nabla.V = \frac{\partial \dot{x}_1}{\partial x_1} + \frac{\partial \dot{x}_2}{\partial x_2} + \frac{\partial \dot{x}_3}{\partial x_3} + \frac{\partial \dot{x}_4}{\partial x_4} = -0.8 - \varepsilon \cosh(x_1) \tag{2}$$

by integrating (2), we obtain a unique solution as follows.

$$V(t) = V(0) \exp[(-0.8 - \varepsilon \cosh(x_1))t] \tag{3}$$

From (3), it is evident that $V(t) \to 0$ exponentially as $t \to \infty$ when $\varepsilon > 0$ regardless of the model state variable. As a result, all trajectories are confined to a space for which its volume is zero; therefore, existing attractors can be chaotic. By applying the transformation $(x_1, x_2, x_3, x_4) \leftrightarrow (-x_1, -x_2, -x_3, -x_4)$ on (1), the solution settles the same. It indicates that (1) is symmetric about the entire coordinate.

3.2. Fixed Points and Stability

To examine the stability of fixed points of (1), we start by solving a system of equations $\dot{x}_1 = \dot{x}_2 = \dot{x}_3 = \dot{x}_4 = 0$. The unique solution $E_0(0, 0, 0, 0)$ represents the equilibrium point of (1). The Jacobian matrix of (1) at E_0 is defined by the following.

$$M = \begin{bmatrix} 0.2\beta_1(1-\varepsilon) & \beta_1 & 0 & 0 \\ \beta_2 & -1 & 1 & 1 \\ 0 & -\beta_3 & 0 & 1 \\ -\beta_4 & 0 & 0 & 0 \end{bmatrix} \tag{4}$$

The characteristic polynomial (det $(M - \lambda I_d) = 0$, with I_d as the identity matrix 4×4) associated with the above Jacobian matrix can be expressed as follows:

$$\lambda^4 + a_3\lambda^3 + a_2\lambda^2 + a_1\lambda + a_0 = 0. \tag{5}$$

with $a_3 = 0.2\beta_1\varepsilon - 0.2\beta_1 + 1$, $a_2 = \beta_3 - 0.2\beta_1 - \beta_1\beta_2 + 0.2\varepsilon\beta_1$, $a_1 = 0.2\varepsilon\beta_1\beta_3 + \beta_1\beta_4 - 0.2\beta_1\beta_3$, and $a_0 = \beta_1\beta_4$. For some ranges of system parameters, the eigenvalues, as well as the stability of fixed point E_0, are summarized in Table 1. In light of this table, fixed point E_0 is unstable and the system is, thus, classified in the category of self-excited systems.

Table 1. Eigenvalues and stability of fixed point E_0 for some set parameters when keeping $\varepsilon = 0.5$.

System Parameters (β_1, β_2, β_3, β_4)	Eigenvalues	Stability
(1, 0.1, 1, 0.1)	$\lambda_{1,2} = 0.07478 \pm 0.3373i$ $\lambda_{3,4} = -0.5248 \pm 0.7498i$	Unstable
(5, 0.5, 5, 0.5)	$\lambda_{1,2} = 0.4458 \pm 1.033i$ $\lambda_{3,4} = -0.6958 \pm 1.221i$	Unstable
(8.5, 0.9, 8, 0.8)	$\lambda_{1,2} = 1.159 \pm 1.088i$ $\lambda_{3,4} = -1.234 \pm 1.081i$	Unstable
(10, 1.5, 10, 1)	$\lambda_{1,2} = 1.755 \pm 0.2848i$ $\lambda_{3,4} = -1.755 \pm 0.2848i$	Unstable
(15, 2, 15, 1.5)	$\lambda_1 = 1.199$, $\lambda_2 = 4.156$, $\lambda_3 = -1.254$, $\lambda_2 = -3.601$	Unstable

4. Numerical Outcomes

4.1. Bifurcation Diagrams and Multistability

(1) is solved numerically by performing the standard fourth-order Runge–Kutta integration algorithm and the Lyapunov exponent the Wolf algorithm at $\Delta t = 10^{-3}$. The system shows complex and diverse dynamics, which indicates bifurcation diagrams according to the parameters of the system β_1 to β_4, respectively. Thus, Figure 1 presents bifurcation diagrams (a_i) and their corresponding spectra of Lyapunov exponents (b_i) for $i = 1$ to 4. From these figures, each parameter has an impact on the dynamics of the system (1). In light of the different spectra of the exponents, all behaviors (periodic, chaotic, and hyperchaotic) are observed according to the nature of the Lyapunov exponents [34]. In particular, the hyperchaotic performance of which a sample is represented in Figure 2a–f by the phase portraits on all planes of coordinates system is observed (see the caption of figures for more details).

By carefully observing the previous bifurcation diagrams, a more or less wide window (by superimposing two datum obtained by increasing and decreasing the values of the control parameter) showing the coexistence of the attractors is highlighted according to the color difference. For the set parameters $\beta_1 = 8.15$, $\beta_2 = 0.8$, $\beta_3 = 12.5$, $\beta_4 = 0.5$, and $\varepsilon = 0.5$, by changing only the original condition $x_1(0)$, a coexistence of three different attractors

(a chaotic attractor that coexists with two other periodic) is observed and presented in Figure 3a–d.

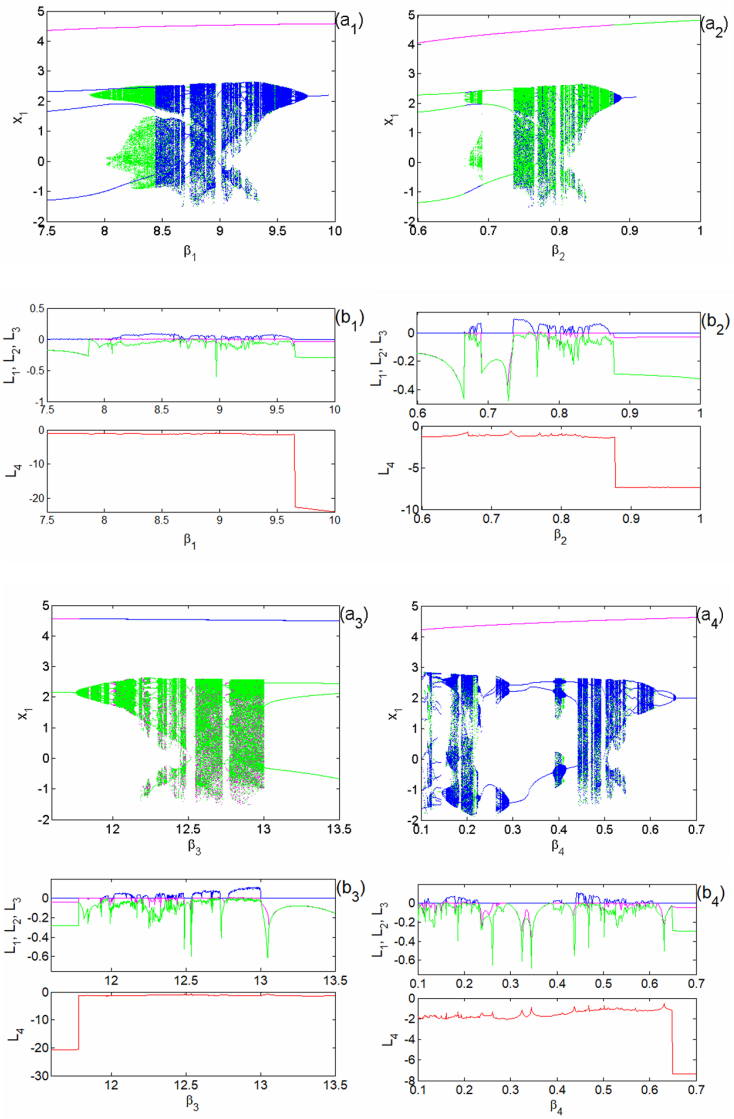


Figure 1. Bifurcation diagrams (a_i) and the corresponding spectra of Lyapunov exponents (b_i) plotted in the different ranges $7.5 \leq \beta_1 \leq 10$, $0.6 \leq \beta_2 \leq 1$, $11.5 \leq \beta_3 \leq 13.5$, and $0.1 \leq \beta_4 \leq 0.7$ for different fixed parameters: (**a1**,**b1**) $\beta_2 = 0.8$, $\beta_3 = 12.5$, $\beta_4 = 0.5$, and $\varepsilon = 0.5$; (**a2**,**b2**) $\beta_1 = 9$, $\beta_3 = 12.5$, $\beta_4 = 0.5$, and $\varepsilon = 0.5$; (**a3**,**b3**) $\beta_1 = 9$, $\beta_2 = 0.8$, $\beta_4 = 0.5$, and $\varepsilon = 0.5$; (**a4**,**b4**) $\beta_1 = 9$, $\beta_2 = 0.8$, $\beta_3 = 12.5$, and $\varepsilon = 0.5$ respectively.

4.2. Raspberry Simulation

Raspberry Pi is a mini-computer that can be connected to a monitor and is used as a standard computer. It is important to note that there are multiple variations of this mini-computer. It needs a minimum number of elements to function and a micro SD memory card compatible with the chosen model, which is used as a hard disk; a keyboard to enter commands; and a monitor to view them. A 5V DC power supply is required to operate the card, not to mention power and connection cables. Raspberry Pi is used for multiple purposes as needed, particularly in computer programming and these related fields [35]. The hyperchaotic oscillator used in this work is solved by using the integration algorithm of Runge–Kutta under a Python programming environment. The phase portrait obtained is observed on the monitor of Figure 4 with a remarkable similarity to that previously observed in Figure 2b.

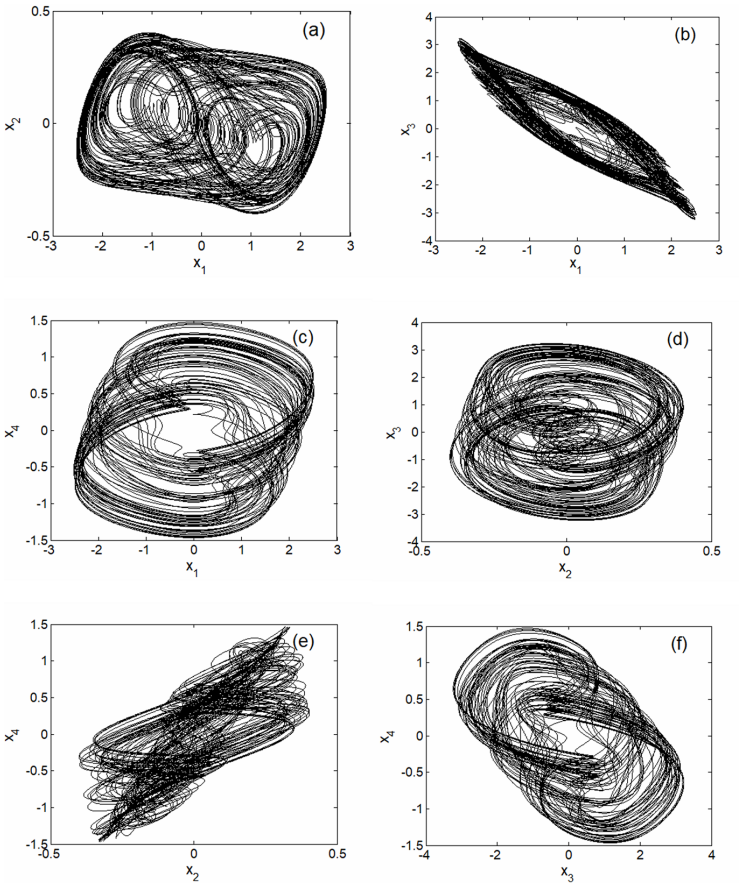


Figure 2. Phase trajectories of the hyperchaotic attractors on system coordinates plane projection for $\beta_1 = 9$, $\beta_2 = 0.759$, $\beta_3 = 12.5$, $\beta_4 = 0.5$, and $\varepsilon = 0.5$.

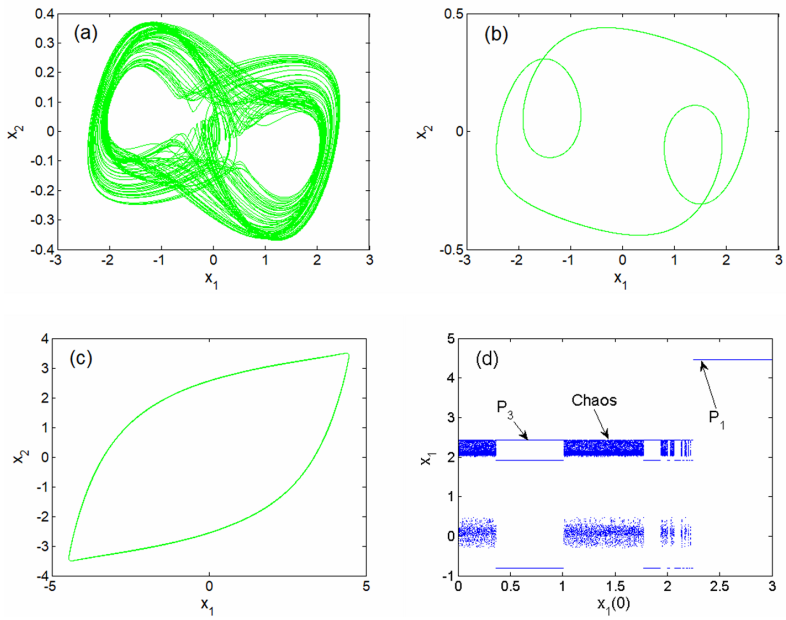
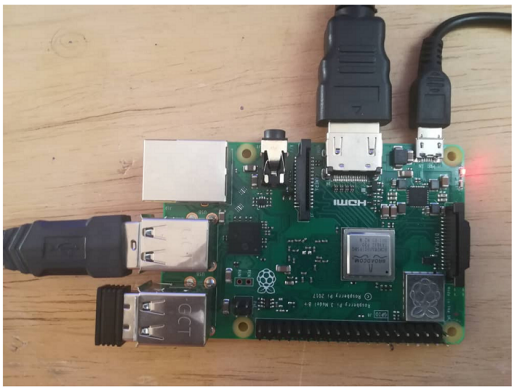
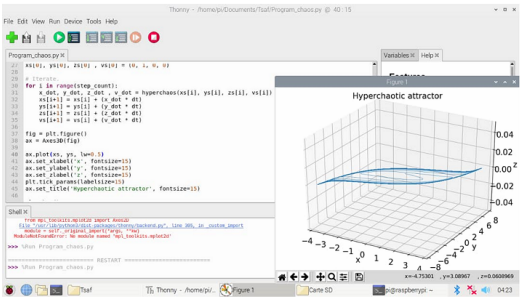


Figure 3. Phase portraits representing the coexistence of four symmetric attractors (chaotic (**a**) and cycle limit of period-3 (**b**) and period-1 (**c**)) and bifurcation such as the sequence showing the local maxima of the coordinate $x_1$versus initial state $x_1(0)$ plotted in the range $0 \leq x_1(0) \leq 3$ obtained for the set parameters $\beta_1 = 8.15$, $\beta_2 = 0.8$, $\beta_3 = 12.5$, $\beta_4 = 0.5$, and $\varepsilon = 0.5$. Initial conditions are $(0.2, 0, 0, 0)$, $(0.8, 0, 0, 0)$, $(2.5, 0, 0, 0)$, and $(x_1(0), 0, 0, 0)$, respectively.



(a)



(b)

Figure 4. The Raspberry Pi card used in operation (**a**); the chaotic portrait obtained by raspberry simulations (**b**).

5. Adaptive Synchronization

In this section, the adaptive synchronization of the hyperchaotic system (1) with unknown parameters newly introduced is discussed. Thus, the master system is considered as follows.

$$\begin{cases} \dot{x}_1 = \beta_1(x_2 + 0.2(x_1 - \varepsilon \sinh(x_1))) \\ \dot{x}_2 = \beta_2 x_1 - x_2 + x_3 + x_4 \\ \dot{x}_3 = -\beta_3 x_2 + x_4 \\ \dot{x}_4 = -\beta_4 x_1 \end{cases} \tag{6}$$

The introduced model is hyperchaotic for $\beta_1 = 9$, $\beta_2 = 0.759$, $\beta_3 = 12.5$, $\beta_4 = 0.5$, and $\varepsilon = 0.5$. The slave system of the previous system is given by the following:

$$\begin{cases} \dot{y}_1 = \beta_1(y_2 + 0.2(y_1 - \varepsilon \sinh(y_1))) + u_1 \\ \dot{y}_2 = \beta_2 y_1 - y_2 + y_3 + y_4 + u_2 \\ \dot{y}_3 = -\beta_3 y_2 + y_4 + u_3 \\ \dot{y}_4 = -\beta_4 y_1 + u_4 \end{cases} \tag{7}$$

where u_i and $(i = 1, 2, 3, 4)$ are the adaptive controls to be designed to ensure the synchronization of the coupled oscillators. The complete synchronization error is defined as follows.

$$e_i = y_i - x_i \tag{8}$$

Then, the error dynamics is expressed as follows.

$$\begin{cases} \dot{e}_1 = \beta_1(e_2 + 0.2(e_1 - \varepsilon(\sinh(y_1) - \sinh(x_1)))) + u_1 \\ \dot{e}_2 = \beta_2 e_1 - e_2 + e_3 + e_4 + u_2 \\ \dot{e}_3 = -\beta_3 e_2 + e_4 + u_3 \\ \dot{e}_4 = -\beta_4 e_1 + u_4 \end{cases} \tag{9}$$

The adaptive control functions $u_1(t)$, $u_2(t)$, $u_3(t)$, and $u_4(t)$ are defined as follows:

$$\begin{cases} u_1 = \beta_1(e_2 + 0.2(e_1 - \varepsilon(\sinh(y_1) - \sinh(x_1)))) - k_1e_1 \\ u_2 = \hat{\beta}_2e_1 - e_2 + e_3 + e_4 - k_2e_2 \\ u_3 = -\hat{\beta}_3e_2 + e_4 - k_3e_3 \\ u_4 = -\hat{\beta}_4e_1 - k_4e_4 \end{cases} \tag{10}$$

where $\hat{\beta}_2$, $\hat{\beta}_3$, and $\hat{\beta}_4$ are estimates of the parameters β_2, β_3, and β_4, respectively, and k_i (i = 1, 2, 3, 4) are positive constants. Substituting the control law (10) into (9), the closed-loop error dynamics are obtained as follows.

$$\begin{cases} \dot{e}_1 = -k_1e_1 \\ \dot{e}_2 = (\beta_2 - \hat{\beta}_2)e_1 - k_2e_2 \\ \dot{e}_3 = -(\beta_3 - \hat{\beta}_3)e_2 - k_3e_3 \\ \dot{e}_4 = -(\beta_4 - \hat{\beta}_4)e_1 - k_4e_4 \end{cases} \tag{11}$$

From (11), the errors of parameter estimations are defined as follows.

$$e_{\beta_2} = \beta_2 - \hat{\beta}_2, e_{\beta_3} = \beta_3 - \hat{\beta}_3, \text{ and } e_{\beta_2} = \beta_4 - \hat{\beta}_4 \tag{12}$$

Substituting (12) into (11), the error dynamics simplifies into the following.

$$\begin{cases} \dot{e}_1 = -k_1e_1 \\ \dot{e}_2 = e_{\beta_2}e_1 - k_2e_2 \\ \dot{e}_3 = -e_{\beta_3}e_2 - k_3e_3 \\ \dot{e}_4 = -e_{\beta_4}e_1 - k_4e_4 \end{cases} \tag{13}$$

The candidate quadratic Lyapunov function is a positive function on $\Re^7$ that can be defined as the following:

$$V(e_i, e_{\beta_2}, e_{\beta_3}, e_{\beta_4}) = \frac{1}{2}\left(e_1^2 + e_2^2 + e_3^2 + e_4^2 + e_{\beta_2}^2 + e_{\beta_3}^2 + e_{\beta_4}^2\right). \tag{14}$$

where (i = 1, 2, 3, 4). With $\dot{e}_{\beta_2} = -\dot{\hat{\beta}}_2$, $\dot{e}_{\beta_3} = -\dot{\hat{\beta}}_3$, and $\dot{e}_{\beta_2} = -\dot{\hat{\beta}}_4$, the derivative function along the trajectories of (14) is obtained by the following.

$$\dot{V} = -k_1e_1^2 - k_2e_2^2 - k_3e_3^2 - k_4e_4^2 + e_{\beta_2}\left(\dot{\hat{\beta}}_2 - e_1e_2\right) - e_{\beta_3}\left(\dot{\hat{\beta}}_3 + e_2e_3\right) + e_{\beta_4}\left(\dot{\hat{\beta}}_3 + e_1e_4\right) \tag{15}$$

From (15), the determined parameters are modernized according to the following law.

$$\begin{cases} \dot{\hat{\beta}}_2 = e_1e_2 + k_5e_{\beta_2} \\ \dot{\hat{\beta}}_3 = -e_2e_3 + k_6e_{\beta_3} \\ \dot{\hat{\beta}}_4 = -e_1e_4 + k_7e_{\beta_4} \end{cases} \tag{16}$$

Substituting (16) into (15), we obtain the following.

$$\dot{V} = -k_1e_1^2 - k_2e_2^2 - k_3e_3^2 - k_4e_4^2 - k_5e_{\beta_2}^2 - k_6e_{\beta_3}^2 - k_7e_{\beta_4}^2 \tag{17}$$

This shows that $\dot{V}$ is a negative specific function on $\Re^7$. Thus, by Lyapunov stability theory [36], it is essential that the synchronization error and the parameter error decay to zero exponentially with time for all primary conditions. Hence, the following outcomes are established.

The parameter values of the master and response hyperchaotic dynamics are chosen as follows: for $\beta_1 = 9$, $\beta_2 = 0.759$, $\beta_3 = 12.5$, $\beta_4 = 0.5$, and $\varepsilon = 0.5$; the constants $k_i(i = 1...7) = 1$. In addition, the initial conditions of the master system are fixed as follows: $x_1(0) = 0.2$, $x_2(0) = 0$, $x_3(0) = 0$, and $x_4(0) = 0$; the ones for the slave system are fixed as

$y_1(0) = 1$, $y_2(0) = 0.3$, $y_3(0) = 0.5$, and $y_4(0) = 1$. The primary values of the determined parameters are $\hat{\beta}_2(0) = 0.1$, $\hat{\beta}_3(0) = 0.03$, and $\hat{\beta}_4(0) = 0.01$.

The complete synchronization of the different master and slave system states is described in Figure 5. Figure 6 displays that the determined values of parameters $\hat{\beta}_2$, $\hat{\beta}_3$, and $\hat{\beta}_4$ converge to system parameters $\beta_2 = 3$, $\beta_3 = 4.5$, and $\beta_4 = 1$.

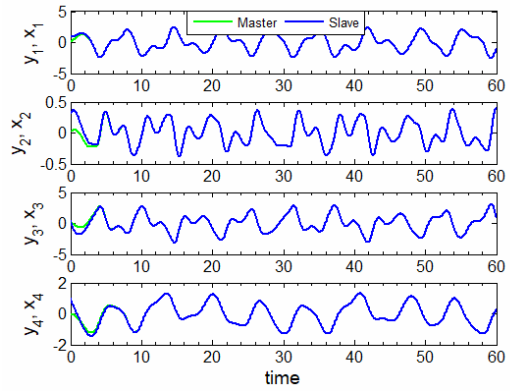


Figure 5. Adaptive synchronization of the master and slave systems.

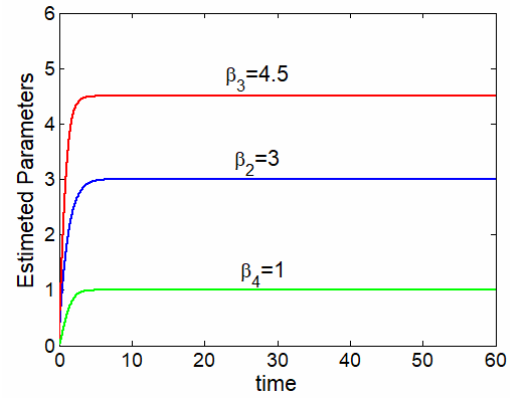


Figure 6. Evolution of the estimated parameters $\hat{\beta}_2$, $\hat{\beta}_3$, and $\hat{\beta}_4$.

6. Proposed Image Encryption Algorithm

6.1. Key Generation

A hash function called SHA-256 is applied to the input image to produce the secret key of (1), (x_0, y_0, z_0, w_0). It generates a hash value of 256-bit, which behaves as the signature of the image. Accordingly, for two pristine images that are distinct in one bit, the corresponding hash values and the corresponding secret keys are dissimilar. The 204 first bits of the hash value are divided into four sub-sequences with the same length of 51 bits. The decimal representations of these sub-sequences are referred to as h_1, h_2, h_3, and h_4. The secret key of (1) is obtained by (18)–(21).

$$x_1 = \frac{1}{2}(x_0 + h_1) \bmod 3 \tag{18}$$

$$y_1 = \frac{1}{2}(y_0 + h_2) \bmod 3 \tag{19}$$

$$z_1 = \frac{1}{2}(z_0 + h_3) \bmod 3 \tag{20}$$

$$w_1 = \frac{1}{2}(w_0 + h_4) \bmod 3 \tag{21}$$

6.2. Encryption Procedure

In this part, the stepwise of the presented image cryptosystem, shown in Figure 7, is provided. It consists of two main phases, i.e., pixel-based permutation and bit-wise diffusion:

1. Pixel-based permutation phase: the original image **P** of size $M \times N$ undergo a permutation operation that works at the pixel level as given below.
   - Iterate (1) $M \times N/4$ times with the control parameters $(\beta_1, \beta_2, \beta_3, \beta_4, \varepsilon)$ and the initial conditions (x_1, y_1, z_1, w_1) (cf. (18)–(21)), which yields four chaotic matrices **X**, **Y**, **Z**, and **W** each of size $M \times N/4$;
   - Concatenate matrices **X**, **Y**, **Z**, and **W** into a matrix **V** of size $M \times N$. Then, map **V** from $[0, 3]$ to $\{0, 1, 2, \ldots, 255\}$ using (22), which produced a matrix **S**:

$$S = \left[\left(V \times 10^{15} \right) \bmod 256 \right], \tag{22}$$

     where $[x]$ refers the integer part of x;
   - Transform matrix **S** into a sequence **s** of length MN. The elements of **s** are then arranged in ascending order to generate a new sequence denoted by $\mathbf{s}_1$. Let **r** be an array that contains the indices of the elements of **s** in $\mathbf{s}_1$;
   - After resizing the original image **P** into a sequence **p** of length MN, the permuted process is applied as follows;

$$p_r(i) = p(r(i)) \quad i = 1, 2, \ldots, MN \tag{23}$$

   - Next, we reshape $\mathbf{p}_r$ into $\mathbf{P}_1$, an $M \times N$ matrix. In short, the permutation process can be referred to as follows.

$$P_1 = F_r(P) \tag{24}$$

2. Bit-wise diffusion: Apply the diffusion function g_s to the elements of $\mathbf{P}_1$ using **S** as follows:

$$C = P_1 \oplus S, \tag{25}$$

   where $\oplus$ indicates the bit-wise XOR process and **C** is the encrypted image. Simply, the diffusion process can be formulated as follows.

$$C = G_S(P_1) \tag{26}$$

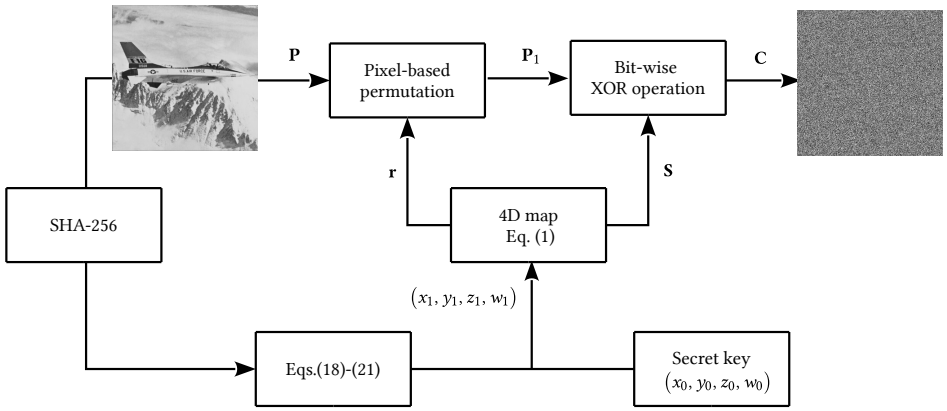


Figure 7. Block diagram of the proposed encryption algorithm.

6.3. Decryption Procedure

The decryption is usually a reverse of the encryption process. The decryption scheme corresponding to the proposed encryption approach is displayed in Figure 8. The presented algorithm is symmetric, which means that it utilizes the same cryptographic keys for both encryption of plaintext and decryption of ciphertext. Accordingly, the secret key of (1) (cf. (x_0, y_0, z_0, w_0)) along with the hash value of the pristine image should be communicated

to the decryption part. By applying (18)–(21), the receiver produces the correct secret key and can then recover the original image by using (27):

$$D = F_r^{-1}(G_S(C)), \tag{27}$$

where **D** is the decrypted image, and $F_{\mathbf{r}}^{-1}$ denotes the inverse function of $F_{\mathbf{r}}$.

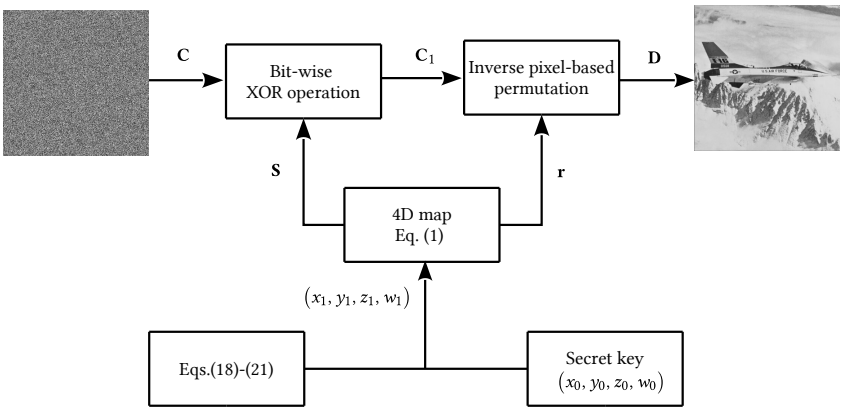


Figure 8. Block diagram of the proposed decryption algorithm.

7. Performance and Security Analysis

7.1. Keyspace Analysis

The keyspace of the proposed scheme consists of the 256-bit hash value of the pristine image and the primary conditions of (1), i.e., (x_0, y_0, z_0, w_0). Suppose that the double-precision datatype used is the 51-bit floating-point format. The possible values of x_0 are more comprehensive than 51 bits, as are the values of y_0, z_0, and w_0. The security claim of the best possible collision attack on the SHA-256 hash function is 2^{128}. Consequently, the keyspace of the proposed algorithm is larger than 332 bits, which is sufficient against brute-force attacks.

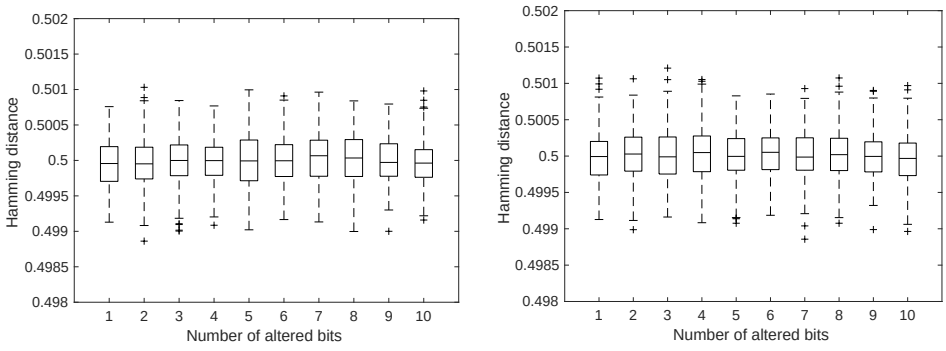
7.2. Sensitivity Analysis

7.2.1. Key Sensitivity

A secure cryptosystem should be highly sensitive to even the slight changes in the secret key. Therefore, modifying a few bits in the secret key should completely alter the cipher image or the original image in case of decryption. Figure 9a depicts the result of hamming distance versus several altered bits of the proposed encryption scheme. To conduct this test [37], the indices n ($n = 1, \cdots, 10$) of the modified bits and the 512×512 test images are generated randomly for 200 iterations. It is noted that the hamming distance is very close to the optimum value of 0.5, even for a single bit alteration in the key. Consequently, the suggested approach is highly sensitive to the slight variations in the secret keys.

7.2.2. Plaintext Sensitivity

Plaintext sensitivity refers to the change in the encrypted image with a single bit variation in the original image. Encryption schemes with better plaintext sensitivity are robust against chosen-plaintext attacks. Figure 9b depicts the plot of hamming distances versus the number of modified bits in the plain image [37]. The indices n ($n = 1, \cdots, 10$) of the modified bits and the 512×512 images are generated randomly under 200 iterations. It can be observed that with the proposed algorithm, the hamming distances are quite close to the optimum value of 0.5, even with the modification of a single bit in the original image. Hence, we can infer that the proposed approach is extremely sensitive to the minor modification in the pristine image.



(**a**) (**b**)

Figure 9. Key sensitivity (**a**) and plaintext sensitivity (**b**) for the proposed cryptosystem, where $x_0 = 1.167504546665441$, $y_0 = 0.531351156161691$, $z_0 = 1.264565351928468$, and $w_0 = 2.697465174434910$.

7.2.3. NPCR and UACI tests

In a secure image cryptosystem, the cipher image is susceptible to minor modifications in the plain image. There are two well-known quantitative measures, namely UACI (Unified Average Changing Intensity) and NPCR (Number of Pixel Change Rate), employed to test sensitivity. UACI measures the difference in the average intensity while NPCR evaluates the number of distinct pixels. The equations for computing the NPCR and UACI are as follows:

$$\texttt{NPCR} = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}\mathcal{D}(i,j), \tag{28}$$

$$\texttt{UACI} = \frac{1}{255 \times MN}\sum_{i=1}^{M}\sum_{j=1}^{N}|\mathbf{C}_1(i,j) - \mathbf{C}_2(i,j)|, \tag{29}$$

where M and N are the rows and columns in the image, respectively, and $\mathcal{D}(i,j)$ refers to the difference between $\mathbf{C}_1$ and $\mathbf{C}_2$, given by the following equation.

$$\mathcal{D}(i,j) = \begin{cases} 0, & \text{if } \mathbf{C}_1(i,j) = \mathbf{C}_2(i,j) \\ 1, & \text{if } \mathbf{C}_1(i,j) \neq \mathbf{C}_2(i,j) \end{cases}$$

Table 2 displays the comparative results of the mean and the variance of UACI and NPCR employed on many grayscale images. It can be observed that the mean value of the NPCR and the UACI exceed 99.6% and 33.46%, respectively, which indicates high sensitivity to the smaller variations in the original image pixels. Consequently, the encrypted scheme can produce entirely different cipher images even with a single bit difference in the two source images.

Table 2. NPCR and UACI (mean and variance) of the ciphered images with a single-bit alteration in the pristine image.

	NPCR (%)				**UACI (%)**			
	[38]	[39]	[40]	Proposed	[38]	[39]	[40]	Proposed
Mean	99.6103	99.6100	99.2000	99.6095	33.4674	33.4526	31.9249	33.4615
Variance	0.0002	0.0002	0.0926	0.0002	0.0018	0.0020	0.4232	0.0019

7.3. Statistical Analysis

7.3.1. Bit Distribution within Each Bit-Plane

Grayscale image pixels are ordinarily represented in 8-bits; hence, an image comprises eight bit-planes. The authors in [41] demonstrated that bit-planes corresponding to the most

significant bits (MSBs) are highly correlated in the original images. Intruders can exploit this fact to retrieve a considerable number of bits in higher bit-planes by comprehending its neighboring bit-plane. Consequently, each bit plane in the cipher image should be highly uniform in terms of bit distribution. The uniformity is measured in the percentage of 1's and 0's in the bit-planes (expected value 50%). Table 3 shows the bit distributions of the original images and their encrypted counterparts. It can be observed that the mean of the bit uniformity in all the bit-planes is quite close to 50% in the encrypted images. The algorithm also exhibits almost identical variances in the percentage of 1's with values close to zero.

Table 3. Percentage of 1's (mean and variance) in several pristine images vs. their encrypted equivalents for the presented scheme

		8th Bit	7th Bit	6th Bit	5th Bit	4th Bit	3rd Bit	2nd Bit	1st Bit
Mean	Orig.	79.0880	20.9120	73.4399	26.5601	67.6198	32.3802	63.9955	36.0045
	Encr.	50.0189	49.9811	49.9823	50.0177	49.9874	50.0126	50.0090	49.9910
Variance	Orig.	503.1185	503.1185	273.1839	273.1839	243.3089	243.3089	231.2194	231.2194
	Encr.	0.0080	0.0080	0.0092	0.0092	0.0096	0.0096	0.0102	0.0102

Orig. refers to the original images and Encr. refers to the encrypted ones.

7.3.2. Correlation analysis

Adjacent pixels are highly correlated in the original images. This is because the neighboring pixel values are very close to each other in natural images. Cryptanalysts can exploit this feature to break the cipher. Therefore, neighboring pixels in the cipher image should be highly uncorrelated. Cryptanalysts can use this feature to break the cipher. The correlation coefficient between any two pixels in an image is calculated by utilizing the following equation:

$$C_{ab} = \frac{\sum_{i=1}^{K}(a_i - \mathbb{E}\{a\})(b_i - \mathbb{E}\{b\})}{\sqrt{\sum_{i=1}^{K}(a_i - \mathbb{E}\{a\})^2}\sqrt{\sum_{i=1}^{K}(b_i - \mathbb{E}\{b\})^2}}, \tag{30}$$

where a_i and b_i denote grayscale values of the neighboring pixels, K is the total number of pixels taken for the calculation, and $\mathbb{E}\{.\}$ indicates the expected values of the random variables. Table 4 displays the mean values of the correlation coefficients between adjacent pixels in the horizontal, vertical, and diagonal directions. We have taken 3000 random samples each from the plain and the cipher images in these directions. It can be observed from the table that the mean values of the correlation coefficient in the cipher images in all three directions are pretty close to zero. Therefore, adjacent pixels in the ciphered image's horizontal, vertical, and diagonal directions are highly uncorrelated. Figure 10 shows this property graphically where the plots of the adjacent pixel correlation of the pristine image per direction are shown in Figure 10a–c, respectively. On the other hand, plots of their encrypted counterparts are presented in Figure 10d–f. The encryption scheme satisfies the requirement of almost zero correlation, making it resistant to various correlation-based attacks.

Table 4. Average of the absolute values of the correlation between neighboring pixel pairs in the pristine and ciphered images.

Scan Direction	Original Images	Encrypted Images
Hor.	0.9868	0.0021
Ver.	0.9889	0.0019
Dia.	0.9781	0.0021

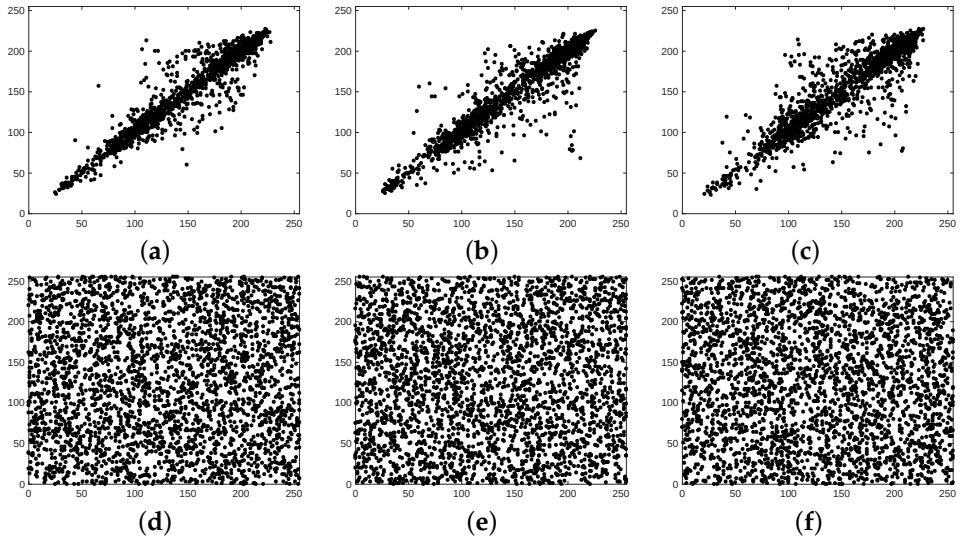


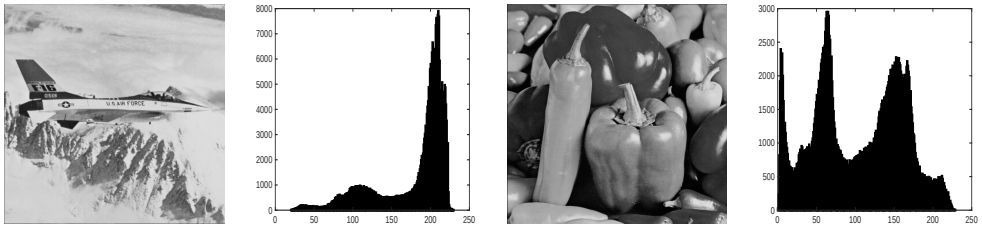
Figure 10. Distribution of adjacent pixel pairs in the pristine and ciphered images of Airplane. Distributions of two horizontally (**a**), vertically (**b**), and diagonally (**c**) neighboring pixels in the original image. Distributions of two horizontally (**d**), vertically (**e**), and diagonally (**f**) neighboring pixels in the encrypted image.

7.3.3. Histogram and Chi-Square Test

The histogram of an image graphically describes the distribution of pixel intensities in the image. Original images usually have non-uniform histograms because pixel intensities are limited within some range. This property can be exploited by cryptanalysts to intercept the cipher using histogram-based attacks. Therefore, a secure encryption scheme should produce cipher images with uniform histograms. Figure 11 shows two grayscale images, namely Airplane and Peppers, along with their histograms, while Figure 12 depicts the encrypted analogs of the original images along with their histograms. It can be observed that the original images exhibit non-uniform histograms while encrypted images have highly uniform distributions of pixel intensities. Histogram uniformity is usually characterized by the Chi-square test [42] quantitatively and computed using the following equation:

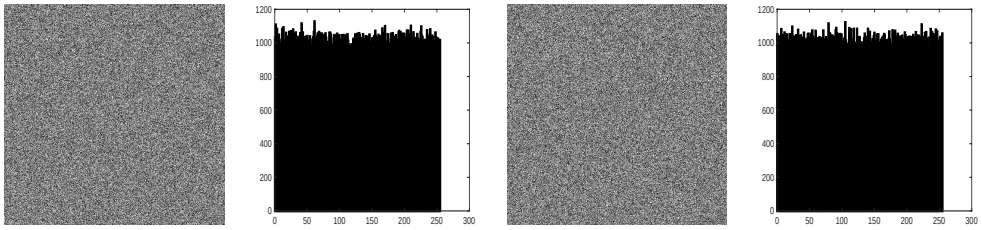
$$\chi^2 = \sum_{i=0}^{L_p-1} \frac{(o_i - e_i)^2}{e_i}, \tag{31}$$

where L denotes the total number of pixel levels, o_i indicates the frequency of occurrence of a particular pixel value (within 0–255) in the histogram, and e_i denotes the predicted frequency of occurrence in the uniform distribution given by $e_i = (M \times N)/256$. The distribution in the experiment is considered to be uniform such that, when the p-value is found to be more than a significance level s ($s \in [0, 1]$), the null hypothesis is accepted. p-value is the probability that summarizes the randomness strength of a test sample against the perfect sample in the experiment. A zero p-value indicates the least randomness and, hence, least amount of uniformity in the histogram, while a value more than 0.01 corresponds to sufficient randomness and uniformity. Table 5 shows the comparison of the mean, variance, and the success rate of the chi-square test (p-value) of different encryption schemes. The mean of the p-value is the highest (0.5339) in the proposed scheme with the success rate of 97%. Hence, the proposed encryption is found to have a uniform histogram and is robust against histogram-based attacks.



(**a**) (**b**) (**c**) (**d**)

Figure 11. Original images of (**a**) Airplane and (**c**) Peppers images; their histograms (**b**) and (**d**), respectively.



(**a**) (**b**) (**c**) (**d**)

Figure 12. Ciphered images of (**a**) Airplane and (**c**) Peppers images; their histograms (**b**) and (**d**), respectively.

Table 5. Chi-square test of the histograms (variance, success rate, and mean) for various image cryptosystems.

	χ^2 **Test (*p*-Value)**			
	[38]	**[39]**	**[40]**	**Proposed**
Mean	0.5115	0.5113	0.3661	0.5339
Variance	0.0837	0.0781	0.0958	0.0746
Success rate (%)	95	96	77	97

7.3.4. Global Entropy

Global entropy is the statistical test for calculating randomness in a sequence, defined as given in (32):

$$H(X) = -\sum_{i=1}^{K} p(x_i)\log_2(p(x_i)) \quad \text{[bits]}, \tag{32}$$

where $p(x_k)$ denotes the occurrence probability of the symbol x_k, and K is the number of different symbols generated by source X. The ideal entropy for an encrypted image is obtained when all pixel levels appear with an equal probability showing uniform pixel distribution. The value of ideal entropy is given as log_2^{28} = 8 bits. The comparisons of the mean and the variances of the global entropies of different encryption algorithms are shown in Table 6. It is observed that the mean of the entropy is very close to the optimal value of 8 and also the highest when compared to the other algorithms. The variance is also found to be close to zero and is the lowest among other algorithms.

Table 6. Global entropy analysis (variance and mean).

	Global Entropy			
	[38]	**[39]**	**[40]**	**Proposed**
Mean	7.999300	7.999300	7.986154	7.999306
Variance ($\times 10^{-9}$)	3.814091	3.197235	9646547	3.080179

7.3.5. Local Entropy

The Local Shannon entropy is the qualitative tool of evaluating the randomness in contrast to the global entropy, where randomness is measured quantitatively. The evaluation of the local Shannon entropy is performed according to [37]. The comparison of the mean and variance of the local entropy is displayed in Table 7. The mean of the local entropy is very close to 8 and is the highest as compared to other algorithms. Similarly, the variance is found to be almost equal to zero, which is lower than [39,40] and slightly higher than [38].

Table 7. Local entropy analysis (variance and mean).

	Local entropy			
	[38]	**[39]**	**[40]**	**Proposed**
Mean	7.902454	7.902396	7.832426	7.902484
Variance ($\times 10^{-7}$)	3.048803	3.820000	2080030	3.140462

7.4. Robustness Analysis

7.4.1. Occlusion Attack

When cipher images are transferred through a communication channel, they are prone to data loss. These losses can affect the decryption process completely or partially. The occlusion attack test is employed on the cipher images to measure the strength of the presented cryptosystem in retrieving the plain image. Table 8 shows the comparison of PSNR between the pristine and ciphered image after undergoing the occlusion attack. The tests are conducted with 1/16, 1/8, 1/4, and 1/2 data losses, and it is observed that the suggested algorithm defeats other cryptosystems with the highest PSNR in all cases. Figure 13a–d show the encrypted images with above mentioned losses while Figure 13e–h show analogous ciphered images. It can be observed that much of the visual information is retained even after half of the encrypted image's information is lost. Consequently, the suggested scheme can efficiently withstand occlusion attacks.

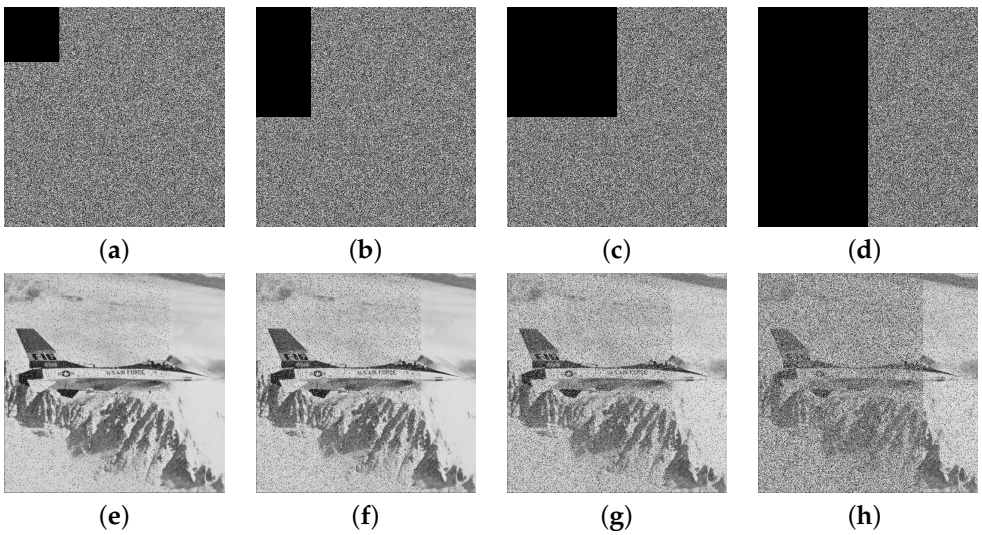


Figure 13. Result of occlusion attacks: ciphered images with (**a**) 1/16, (**b**) 1/8, (**c**) 1/4, and (**d**) 1/2 data loss; corresponding decrypted images (**e**)–(**h**) as per (**a**)–(**d**).

Table 8. The average value of PSNR among pristine and decrypted images resulting from occlusion attacks.

		Occlusion			
	Algorithm	**1/16**	**1/8**	**1/4**	**1/2**
PSNR (dB)	[38]	11.6162	9.6108	8.3915	8.0663
	[39]	8.0552	8.0712	8.0885	8.0723
	[40]	8.4625	8.3750	8.6850	7.9169
	Proposed	20.2283	17.2355	14.1520	11.1497

7.4.2. Noise Attack

Digital images are transferred through various transmission media that are often subjected to the noise present in the channel. This noise can affect the quality of the decrypted image if the corresponding cipher image is subjected to it. To assess the capability of the presented cryptosystem in order to resist such noise attacks, the cipher images are contaminated by the salt and pepper noise with densities 0.005, 0.05, 0.1, and 0.3. Figure 14a–d show the analogous decrypted images. It can be seen from the figures that these images are noisy but still perceivable. Moreover, Table 9 shows the comparison among different algorithms in terms of mean PSNR among the pristine and the decrypted images. The proposed scheme outperforms other algorithms with the highest value of the PSNRs, and it can withstand noise attacks.

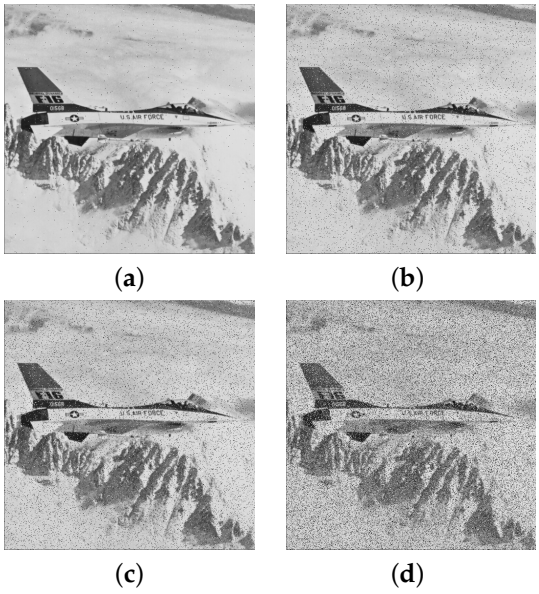


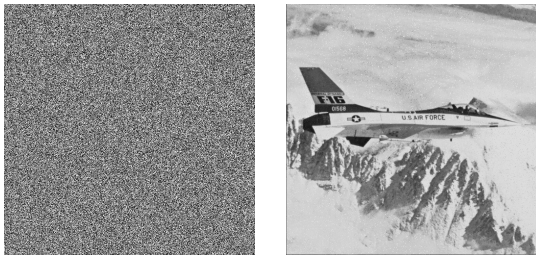
Figure 14. Decrypted images submissive to salt and pepper noise with various noise densities: (**a**) 0.005; (**b**) 0.05; (**c**) 0.100; and (**d**) 0.300.

Table 9. The average value of PSNR among the pristine and decrypted images retrieved from ciphered images that were subjected to salt and pepper noise.

		Density of the Salt and Pepper Noise			
	Algorithm	**0.005**	**0.050**	**0.100**	**0.300**
PSNR (dB)	[38]	21.5400	12.4184	10.1824	8.2172
	[39]	8.0756	8.0452	8.0348	8.0473
	[40]	11.8764	8.3019	8.2093	8.0887
	Proposed	31.2223	21.0743	18.0256	13.2927

7.4.3. Histogram Equalization

Histogram equalization is generally used to increase the image contrast utilizing the histogram of the image. This technique is carried out to make a uniform intensity distribution in the image so that the areas suffering from lower contrast can be transformed to the higher contrast. Figure 15a shows the cipher image under the histogram equalization attack, while Figure 15b depicts the corresponding decrypted image that is slightly blurry but easily recognizable. Moreover, Table 10 reports the comparison among different algorithms in terms of PSNR among the pristine and the decrypted images subjected to the histogram equalization attack. It can be observed that the mean PSNR in the suggested algorithm is more than the schemes in [39,40] while slightly less than [38]. Therefore, the proposed scheme is well capable of handling the histogram equalization attacks.



(**a**) (**b**)

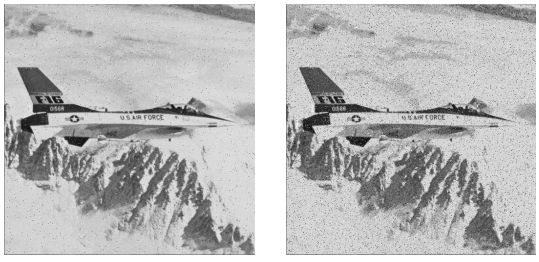
Figure 15. Outcome of histogram equalization attack: (**a**) ciphered image under a histogram equalization attack and (**b**) its decrypted image.

Table 10. The average value of PSNR among pristine and decrypted images retrieved from ciphered images that were subjected to histogram equalization attacks.

	[38]	[39]	[40]	Proposed
PSNR (dB)	39.2943	8.0455	8.0995	32.4690

7.4.4. Contrast Adjustment

Contrast adjustment is performed to modify the contrast of an image using a process called contrast stretching. To perform this operation, pixels with values less than a specified value are usually mapped to the lowest (pure black) value. In contrast, pixels with more than a specific value are fixed to the highest intensity (pure white). Encrypted images can undergo such contrast adjustment attacks causing considerable contamination in the corresponding decrypted images. Figure 16a,b show decrypted images that underwent the contrast adjustment of 20% and 50%, respectively. It can be observed that the recovered images are noisy but easily visible in both cases. Moreover, Table 11 shows a comparison among different algorithms in terms of mean PSNR among the pristine image and the decrypted image, which shows better performance than the schemes proposed in [39,40].



(**a**) (**b**)

Figure 16. Decrypted images under contrast adjustment of (**a**) 20% and (**b**) 50%.

Table 11. The average value of PSNR among the pristine and decrypted images retrieved from ciphered images that were subjected to the contrast adjustment attacks.

		Contrast Increased by a Percentage of	
	Algorithm	**20%**	**50%**
PSNR (dB)	[38]	33.1248	21.0036
	[39]	8.0603	8.0614
	[40]	8.1098	8.0690
	Proposed	26.5443	19.5175

7.5. Classical Attacks

According to Kerkhoff's law of the cryptology [43], assuming all the encryption/decryption algorithms are well known to the attackers, the confidence of the cryptosystem relies only on the secret keys. Cryptanalysts can rebuild the secret key or its equivalent form to decrypt a partial or total content effectively. They can even find a process to recover the pristine image from the cipher image without seeing the key by analyzing the correlations between the encrypted image and the pristine image or the secret key. These search methods resulted in two well-known attacks: the known-plaintext attack and chosen-plaintext attack. A robust cryptosystem should be capable of withstanding these attacks. In the suggested scheme, the SHA256 hash function is adopted to derive the primary values of the hyperchaotic system and its control parameters. Hence, they are sensitive to even a tiny bit of modification in the key and the plain image. This ensures completely different chaotic sequences for the distinctive plain images even if the same secret keys are used. Therefore, a cryptanalyst would not retrieve helpful information about the keys or the decrypted image by analyzing the proposed algorithm. This is because this information highly depends on the input plain image. Consequently, the proposed scheme can resist both the known-plaintext and the chosen-plaintext attacks.

In the case of an attack, the cryptanalysts use all-black and all-white pixel images to make the cipher's substitution and/or permutation processes invalid and infer valuable information. Figure 17 shows the encrypted images and their histograms related to the all-black and all-white images. It is observed that the encrypted images provide no helpful information as they are random-like images, and also, their histograms are quite uniform. The adjacent pixel correlation per direction is displayed in Figure 18 for the all-white and the all-black images, and they all are found to be very close to zero. The p-value in the chi-square test is sufficiently larger to pass the null hypotheses, and the global and the local entropies are very close to the ideal value of 8 for both all-black and the all-white images, as reported in Table 12. Moreover, Table 13 shows that UACI and NPCR values are very close to the typical values of 99.6% and 33.4%, respectively, in both cases. This ensures the ability of the proposed scheme to resist differential attacks effectively. Moreover, the proposed encryption scheme can successfully encipher full-black and full-white images resisting the known and chosen-plaintext attacks.

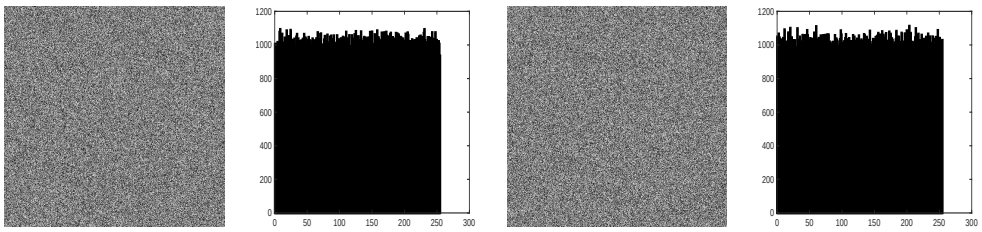


Figure 17. Ciphered images of the (**a**) full-white and (**c**) full-black images; their histograms (**b**) and (**d**), respectively.

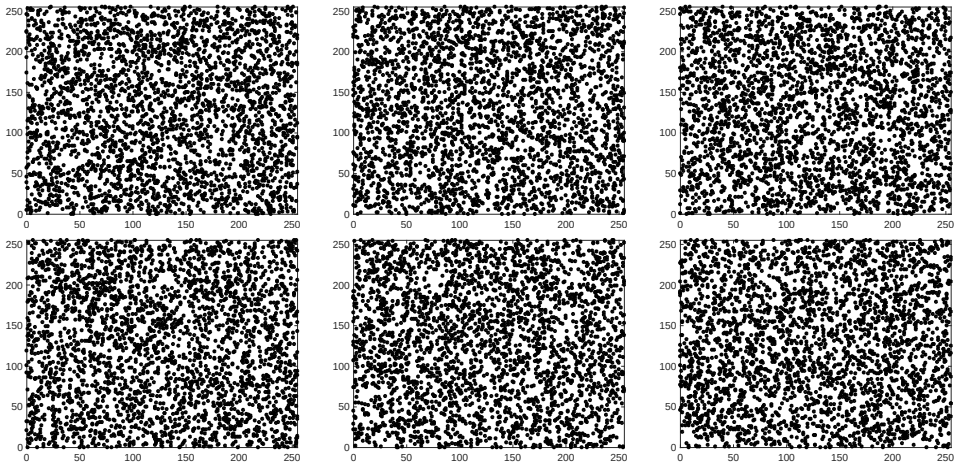


Figure 18. Correlation of neighboring pixel pairs (in the horizontal, vertical, and diagonal directions) for the full-white and full-black images in row-major order.

Table 12. Statistical analyses of ciphered full-white and full-black images.

		χ^2 Test of Histogram	Correlation			Entropy	
Image	**Algorithm**	***p*-Value**	**Hor.**	**Ver.**	**Dia.**	**Global**	**Local**
Full-white	[38]	0.7837	0.0043	−0.0007	0.0003	7.9993	7.9022
	[39]	0.2299	0.0043	0.0028	0.0003	7.9993	7.9030
	[40]	0	0.9991	0.0381	0.0366	3.1642	1.9065
	Proposed	0.8086	0.0022	−0.0009	0.0009	7.9994	7.9015
Full-black	[38]	0	0.0002	−0.0009	0.0046	2.0000	1.9989
	[39]	0	−0.0015	0.0004	−0.0004	0.0384	0.0381
	[40]	0	NaN	NaN	NaN	0.0012	0.0002
	Proposed	0.5935	−0.0048	0.0004	0.0018	7.9993	7.9025

Table 13. Differential analyses of ciphered full-white and full-black images.

Image	**Algorithm**	**NPCR (%)**	**UACI (%)**
Full-white	[38]	99.5861	33.4615
	[39]	99.5983	33.4682
	[40]	62.5015	10.9806
	Proposed	99.6113	33.3647
Full-black	[38]	75.0347	00.4900
	[39]	0.7969	0.0031
	[40]	12.5031	00.0505
	Proposed	99.6227	33.4161

7.6. Time Complexity

A comparison of the time complexity and their magnitude for a 512×512 grayscale image is provided in Table 14. The complexities of the comparative algorithms [38–40] are reported in [37,44]. Table 15 shows a count of frequencies for each elementary operation according to the number of pixels in the image MN. The encryption schemes in [38,39] demand sorting operations. Let v be a vector with l elements; the sorting of a such vector requires, on average, a time complexity of $l \log(l)$ when considered the *quicksort*

algorithm [45]. After collecting the frequencies shown in Table 15 and then disregarding lower-orders terms, the complexity orders are summarized as follows [38–40].

$$\begin{cases} O\left(MN\left(34+\log(L)+2\sqrt{L}\right)\right) \\ O\left(108MN+72L^4\right) \\ O((36n+2)MN) \\ O(65MN+3\times(M+N)) \qquad \text{proposed.} \end{cases} \tag{33}$$

It is observed that the suggested algorithm has the lowest complexity order compared to the ones in [38–40].

Table 14. Orders of time complexity and their magnitude for a grayscale image of dimension $M \times N = 512 \times 512$. For the presented simulation outcomes in [38] and [40], $L = MN$ and $n = 1$, respectively.

Algorithm	Complexity Order	Order of Magnitude ($\times 10^6$)
[38]	$O\left(MN\left(34+\log(L)+2\sqrt{L}\right)\right)$	282
[39]	$O\left(108MN+72L^4\right)$	45
[40]	$O((36n+2)MN)$	10
Proposed	$O((9.25+\log(MN))MN)$	5

Table 15. Time complexity analysis for the suggested image cryptosystem.

Process	Time Complexity
Addition	$1.5MN+4$
Multiplication	$2.5MN+8$
Trigonometric functions	$\frac{MN}{4}$
Mod	$2MN+4$
Rounding functions	MN
XOR	MN
Substitutions	$MN+4$
Sorting vector of length	MN
SHA-256 operations	$\frac{8}{512}MN$

8. Concluding Remarks

Exultant implementation of an image cryptosystem using the randomness of hyperchaotic system with hyperbolic nonlinearity and permutation and substitution operations is presented. First, the system is investigated numerically and analytically for exploration and the selection of hyperchaotic behavior utilized for encryption. From this examination appears a rich dynamic, namely, the existence of a single unstable equilibrium point, the hysteresis phenomenon giving rise to the coexistence of three different attractors, and period-doubling bifurcation. Then, an encryption method is designed by using both the hyperchaotic character well chosen previously and one round of permutation and diffusion operations. The SHA-256 hash value of the original image is used to generate the secret key of the cryptosystem, which renders chosen/known-plaintext attacks impossible. The feasibility and synchronization of the proposed system are also presented by developing, respectively, Raspberry surveys and an adaptive synchronization scheme of two identical hyperchaotic systems. Experiment results were presented to show that the proposed algorithm satisfied all required properties of a secure cryptosystem, in addition to its low complexity and its merit for practical use. Comparisons with some state-of-the-art algorithms demonstrated that the proposed algorithm offers the best performance/complexity

trade-off. In future work, we aim to utilize the presented hyperchaotic system in designing video cryptosystems for the Internet of Things applications.

Author Contributions: Conceptualization, T.N., B.A.-E.-A., M.N.A., A.B., C.V., N.J.D.D. and A.A.A.E.-L.; methodology, T.N., B.A.-E.-A., M.N.A., A.B., C.V., N.J.D.D. and A.A.A.E.-L.; software, T.N., B.A.-E.-A., M.N.A., A.B., C.V., N.J.D.D. and A.A.A.E.-L.; validation, T.N., B.A.-E.-A., M.N.A., A.B., C.V., N.J.D.D. and A.A.A.E.-L. All authors have read and agreed to the published version of the manuscript.

Funding: Ahmed A. Abd El-Latif acknowledges the support of EIAS Data Science Lab, College of Computer and Information Sciences, Prince Sultan University, Riyadh, Saudi Arabia for their support of this research.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The datasets generated and analysed during the current study are available from the corresponding author upon reasonable request.

Acknowledgments: Bassem Abd-El-Atty acknowledges support from Luxor University, Egypt. Ahmed A. Abd El-Latif acknowledges the support of EIAS Data Science Lab, College of Computer and Information Sciences, Prince Sultan University, Riyadh, Saudi Arabia for their support of this research.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Volos, C.; Akgul, A.; Pham, V.T.; Stouboulos, I.; Kyprianidis, I. A simple chaotic circuit with a hyperbolic sine function and its use in a sound encryption scheme. *Nonlinear Dyn.* **2017**, *89*, 1047–1061. [CrossRef]
2. Wang, Y.; Wong, K.W.; Liao, X.; Xiang, T.; Chen, G. A chaos-based image encryption algorithm with variable control parameters. *Chaos Solitons Fractals* **2009**, *41*, 1773–1783. [CrossRef]
3. Mylrea, M. Smart energy-internet-of-things opportunities require smart treatment of legal, privacy and cybersecurity challenges. *J. World Energy Law Bus.* **2017**, *10*, 147–158. [CrossRef]
4. Guan, Z.; Si, G.; Wu, J.; Zhu, L.; Zhang, Z.; Ma, Y. Utility-Privacy Tradeoff Based on Random Data Obfuscation in Internet of Energy. *IEEE Access* **2017**, *5*, 3250–3262. [CrossRef]
5. Awrejcewicz, J.; Krysko, A.V.; Soldatov, V.; Krysko, V.A. Analysis of the Nonlinear Dynamics of the Timoshenko Flexible Beams Using Wavelets. *J. Comput. Nonlinear Dyn.* **2011**, *7*. [CrossRef]
6. Njitacke, Z.T.; Kengne, J.; Fozin, T.F.; Leutcha, B.P.; Fotsin, H.B. Dynamical analysis of a novel 4-neurons based Hopfield neural network: Emergences of antimonotonicity and coexistence of multiple stable states. *Int. J. Dyn. Control* **2019**, *7*, 823–841. [CrossRef]
7. Kengne, J.; Mogue, R.L.T.; Fozin, T.F.; Telem, A.N.K. Effects of symmetric and asymmetric nonlinearity on the dynamics of a novel chaotic jerk circuit: Coexisting multiple attractors, period doubling reversals, crisis, and offset boosting. *Chaos Solitons Fractals* **2019**, *121*, 63–84. [CrossRef]
8. Pham, V.; Jafari, S.; Volos, C.; Fortuna, L. Simulation and experimental implementation of a line–equilibrium system without linear term. *Chaos Solitons Fractals* **2019**, *120*, 213–221. [CrossRef]
9. Jafari, S.; Ahmadi, A.; Panahi, S.; Rajagopal, K. Extreme multi-stability: When imperfection changes quality. *Chaos Solitons Fractals* **2018**, *108*, 182–186. [CrossRef]
10. Kountchou, M.; Signing, V.F.; Mogue, R.T.; Kengne, J.; Louodop, P.; Saïdou. Complex dynamic behaviors in a new Colpitts oscillator topology based on a voltage comparator. *AEU—Int. J. Electron. Commun.* **2020**, *116*, 153072. [CrossRef]
11. Wang, Z.; Wei, Z.; Sun, K.; He, S.; Wang, H.; Xu, Q.; Chen, M. Chaotic flows with special equilibria. *Eur. Phys. J. Spec. Top.* **2020**, *229*, 905–919. [CrossRef]
12. Amin, M.; Abd El-Latif, A.A. Efficient modified RC5 based on chaos adapted to image encryption. *J. Electron. Imaging* **2010**, *19*, 013012. [CrossRef]
13. Belazi, A.; Abd El-Latif, A.A.; Rhouma, R.; Belghith, S. Selective image encryption scheme based on DWT, AES S-box and chaotic permutation. In Proceedings of the 2015 International Wireless Communications and Mobile Computing Conference (IWCMC), Dubrovnik, Croatia, 24–28 August 2015; pp. 606–610.
14. Abd-El-Atty, B.; Abd El-Latif, A.A.; Venegas-Andraca, S.E. An encryption protocol for NEQR images based on one-particle quantum walks on a circle. *Quantum Inf. Process.* **2019**, *18*, 272. [CrossRef]
15. Li, L.; Abd-El-Atty, B.; Abd El-Latif, A.A.; Ghoneim, A. Quantum color image encryption based on multiple discrete chaotic systems. In Proceedings of the 2017 Federated Conference on Computer Science and Information Systems (FedCSIS), Prague, Czech Republic, 3–6 September 2017; pp. 555–559.

16. Abd El-Latif, A.A.; Niu, X.; Amin, M. A new image cipher in time and frequency domains. *Opt. Commun.* **2012**, *285*, 4241–4251. [CrossRef]
17. Abd El-Latif, A.A.; Yan, X.; Li, L.; Wang, N.; Peng, J.L.; Niu, X. A new meaningful secret sharing scheme based on random grids, error diffusion and chaotic encryption. *Opt. Laser Technol.* **2013**, *54*, 389–400. [CrossRef]
18. Migallón, H.; Jimeno-Morenilla, A.; Sánchez-Romero, J.L.; Belazi, A. Efficient parallel and fast convergence chaotic Jaya algorithms. *Swarm Evol. Comput.* **2020**, *56*, 100698. [CrossRef]
19. Kiseleva, M.A.; Kudryashova, E.V.; Kuznetsov, N.V.; Kuznetsova, O.A.; Leonov, G.A.; Yuldashev, M.V.; Yuldashev, R.V. Hidden and self-excited attractors in Chua circuit: Synchronization and SPICE simulation. *Int. J. Parallel Emergent Distrib. Syst.* **2017**, *33*, 513–523. [CrossRef]
20. Signing, V.F.; Kengne, J.; Pone, J.M. Antimonotonicity, chaos, quasi-periodicity and coexistence of hidden attractors in a new simple 4-D chaotic system with hyperbolic cosine nonlinearity. *Chaos Solitons Fractals* **2019**, *118*, 187–198. [CrossRef]
21. Nazarimehr, F.; Sprott, J.C. Investigating chaotic attractor of the simplest chaotic system with a line of equilibria. *Eur. Phys. J. Spec. Top.* **2020**, *229*, 1289–1297. [CrossRef]
22. Njitacke, Z.; Kengne, J.; Fotsin, H.; Negou, A.N.; Tchiotsop, D. Coexistence of multiple attractors and crisis route to chaos in a novel memristive diode bidge-based Jerk circuit. *Chaos Solitons Fractals* **2016**, *91*, 180–197. [CrossRef]
23. Tsafack, N.; Kengne, J. A Novel Autonomous 5-D Hyperjerk RC Circuit with Hyperbolic Sine Function. *Sci. World J.* **2018**, *2018*, 1–17. [CrossRef]
24. Tapche, R.W.; Njitacke, Z.T.; Kengne, J.; Pelap, F.B. Complex dynamics of a novel 3D autonomous system without linear terms having line of equilibria: Coexisting bifurcations and circuit design. *Analog Integr. Circuits Signal Process.* **2020**, *103*, 57–71. [CrossRef]
25. Çavuşoğlu, U.; Panahi, S.; Akgül, A.; Jafari, S.; Kaçar, S. A new chaotic system with hidden attractor and its engineering applications: Analog circuit realization and image encryption. *Analog Integr. Circuits Signal Process.* **2018**, *98*, 85–99. [CrossRef]
26. Norouzi, B.; Seyedzadeh, S.M.; Mirzakuchaki, S.; Mosavi, M.R. A novel image encryption based on row-column, masking and main diffusion processes with hyper chaos. *Multimed. Tools Appl.* **2013**, *74*, 781–811. [CrossRef]
27. Tsafack, N.; Kengne, J.; Abd-El-Atty, B.; Iliyasu, A.M.; Hirota, K.; EL-Latif, A.A.A. Design and implementation of a simple dynamical 4-D chaotic circuit with applications in image encryption. *Inf. Sci.* **2020**, *515*, 191–217. [CrossRef]
28. Tsafack, N.; Iliyasu, A.M.; Dieu, N.J.D.; Zeric, N.T.; Kengne, J.; Abd-El-Atty, B.; Belazi, A.; EL-Latif, A.A.A. A memristive RLC oscillator dynamics applied to image encryption. *J. Inf. Secur. Appl.* **2021**, *61*, 102944. [CrossRef]
29. Zhou, Y.; Bao, L.; Chen, C.P. A new 1D chaotic system for image encryption. *Signal Process.* **2014**, *97*, 172–182. [CrossRef]
30. Wu, X.; Kan, H.; Kurths, J. A new color image encryption scheme based on DNA sequences and multiple improved 1D chaotic maps. *Appl. Soft Comput.* **2015**, *37*, 24–39. [CrossRef]
31. Hua, Z.; Zhou, Y.; Huang, H. Cosine-transform-based chaotic system for image encryption. *Inf. Sci.* **2019**, *480*, 403–419. [CrossRef]
32. Zhang, J.; Lu, Z.; Li, M. Study on an efficient hyper-chaos-based image encryption scheme using global bit permutation. *Technol. Health Care* **2020**, *28*, 303–309. [CrossRef]
33. Liu, L.; Liu, C. Theoretical Analysis and Circuit Verification for Fractional-Order Chaotic Behavior in a New Hyperchaotic System. *Math. Probl. Eng.* **2014**, *2014*, 1–14. [CrossRef]
34. Wolf, A.; Swift, J.B.; Swinney, H.L.; Vastano, J.A. Determining Lyapunov exponents from a time series. *Phys. D Nonlinear Phenom.* **1985**, *16*, 285–317. [CrossRef]
35. Jain, S.; Vaibhav, A.; Goyal, L. Raspberry Pi based interactive home automation system through E-mail. In Proceedings of the 2014 International Conference on Reliability Optimization and Information Technology (ICROIT), Haryana, India, 6–8 February 2014. [CrossRef]
36. Hahn, W. *Stability of Motion*; Springer: Berlin/Heidelberg, Germany, 1967. [CrossRef]
37. Belazi, A.; Talha, M.; Kharbech, S.; Xiang, W. Novel medical image encryption scheme based on chaos and DNA encoding. *IEEE Access* **2019**, *7*, 36667–36681. [CrossRef]
38. Zhou, Y.; Hua, Z.; Pun, C.M.; Chen, C.P. Cascade chaotic system with applications. *IEEE Trans. Cybern.* **2015**, *45*, 2001–2012. [CrossRef]
39. Hua, Z.; Zhou, Y. Design of image cipher using block-based scrambling and image filtering. *Inf. Sci.* **2017**, *396*, 97–113. [CrossRef]
40. Souyah, A.; Faraoun, K.M. Fast and efficient randomized encryption scheme for digital images based on quadtree decomposition and reversible memory cellular automata. *Nonlinear Dyn.* **2016**, *84*, 715–732. [CrossRef]
41. Zhang, W.; Wong, K.w.; Yu, H.; Zhu, Z.l. A symmetric color image encryption algorithm using the intrinsic features of bit distributions. *Commun. Nonlinear Sci. Numer. Simul.* **2013**, *18*, 584–600. [CrossRef]
42. El Assad, S.; Farajallah, M. A new chaos-based image encryption system. *Signal Process. Image Commun.* **2016**, *41*, 144–157. [CrossRef]
43. Stinson, D.R.; Paterson, M. *Cryptography: Theory and Practice*; CRC Press: Boca Raton, FL, USA, 2018.
44. Aslam, M.N.; Belazi, A.; Kharbech, S.; Talha, M.; Xiang, W. Fourth Order MCA and Chaos-based Image Encryption Scheme. *IEEE Access* **2019**, *7*, 66395–66409.
45. Hoare, C.A.R. Algorithm 64: Quicksort. *Commun. ACM* **1961**, *4*, 321. [CrossRef]