Complex dynamical behaviors of a novel exponential hyper–chaotic system and its application in fast synchronization and color image encryption

Javad Mostafaee¹, Saleh Mobayen¹,²,³, Behrouz Vaseghi¹,⁴, Mohammad Vahedi¹ and Aref Fekih¹,⁵
¹Department of Electrical Engineering, Saveh Branch, Islamic Azad University, Saveh, Iran
²Future Technology Research Center, National Yunlin University of Science and Technology, Douliou, Yunlin, R.O.C
³Department of Electrical Engineering, University of Zanjan, Zanjan, Iran
⁴Department of Electrical Engineering, Abhar Branch, Islamic Azad University, Abhar, Iran
⁵Department of Electrical and Computer Engineering, University of Louisiana at Lafayette, Lafayette, LA, USA

Abstract
This paper proposes a novel exponential hyper–chaotic system with complex dynamic behaviors. It also analyzes the chaotic attractor, bifurcation diagram, equilibrium points, Poincare map, Kaplan–Yorke dimension, and Lyapunov exponent behaviors. A fast terminal sliding mode control scheme is then designed to ensure the fast synchronization and stability of the new exponential hyper–chaotic system. Stability analysis was performed using the Lyapunov stability theory. One of the main features of the proposed controller is the finite time stability of the terminal sliding surface designed with high–order power function of error and derivative of error. The approach was implemented for image cryptosystem. Color image encryption was carried out to confirm the performance of the new hyper–chaotic system. For image encryption, the DNA encryption–based RGB algorithm was used. Performance assessment of the proposed approach confirmed the ability of the proposed hyper–chaotic system to increase the security of image encryption.

Keywords

Corresponding author:
Saleh Mobayen, Future Technology Research Center, National Yunlin University of Science and Technology, 123 University Road, Section 3, Douliou, Yunlin 64002, R.O.C.
Email: mobayens@yuntech.edu.tw

Creative Commons Non Commercial CC BY-NC: This article is distributed under the terms of the Creative Commons Attribution-NonCommercial 4.0 License (https://creativecommons.org/licenses/by-nc/4.0/) which permits non-commercial use, reproduction and distribution of the work without further permission provided the original work is attributed as specified on the SAGE and Open Access pages (https://us.sagepub.com/en-us/nam/open-access-at-sage).
Hyper–chaotic system, chaotic analysis, fast synchronization, terminal sliding mode control, color image encryption

Introduction

Nowadays, we are in a brilliant era of digital communication, where millions of digital images are transmitted and stored on the internet. Digital images play an important role in multimedia images and is widely applied in military, political, commercial, medical, and other fields, which have high confidentiality requirements. Meanwhile, information security becomes a factor that cannot be ignored. It is imperative that the security of digital images with tremendous quantities of information should be guaranteed by reliable techniques. One way to increase data and image communication, is through robust control and encryption using chaotic functions.

Chaotic systems have various characteristics such as highly perceptive of initial state, pseudo randomness, and unpredictability. Two key features of these systems are their uncertainties in the system parameters, and extreme sensitivity to very small changes in their initial conditions. Chaotic programs and methods of analysis were developed over the years. Given that chaotic systems are unpredictable, this key feature can be used in many fields such as: image encryption, robotic, biological networks, neuroscience, secure communication, and information processing. The research on chaotic systems has achieved considerable progress. Many new 3D chaotic systems were adopted, among them the Chen and Ueta, Lü and Chen, and Qi et al. systems, which are generic. This is due to the fact that they are simple in structure and have only one Lyapunov exponent, these chaotic systems have faults of feeble security which make them easily cracked. An important difference between chaotic and hyper–chaotic systems is the fact that high–order hyper–chaotic systems have more complex behavior and higher volatility. The design of high–order chaotic and hyper–chaotic systems along with the analysis of their intrinsic properties and the stability analysis of these systems are among the studies that have been conducted in this field. Dong et al. a high–volatility 4D hyper–chaotic system was introduced. The various states of the system were then analyzed with respect to changes in the system’s equilibrium points. It was confirmed that the more sensitive the system is to the change in the initial conditions, the higher the oscillations. In recent years, many hyper–chaotic systems have been built using various functions, including exponential function, sign function, and trigonometric function. The common features of all these designed systems, compared to conventional hyper–chaotic systems, are their greater fluctuation and their sensitivity to the initial conditions. A four-wing hidden attractor chaotic system, which only has one stable node-focus equilibrium point was reported Deng et al. The new system can generate a hidden attractor with one-wing and hidden attractors with quasi-periodic and periodic coexistence. In addition, by adjusting the parameters of the new system, a self-excited attractor with one wing, is created. The hidden attractions of the new system are confirmed by...
the cross section of the adsorption basins and the hidden behavior is analyzed by selecting different initial states. The dynamic properties of the new system have been proven by the Lyapunov exponents spectrum, bifurcation diagram and Poincare map. Finally, the novel hidden attractor system with four-wings and one-wing has been implemented by electronic circuits. The obtained results showed that the new system has a complex structure and a good performance.

To create a hyper–chaotic system, it is necessary to increase the system dimension, however, this may lead to instability. In a chaotic secure communication system, to ensure secure message transmission, similar systems must be used on both sides of the master and the slave. In order to have a complete and successful transmission, chaotic systems in the master–slave must be synchronized. Dynamic synchronization of these systems, is a very important phenomenon, which has been displayed in many scientific structures. The synchronization of chaotic system’s is a major control approach that has been considered for many years. For synchronization, an appropriate control technique is employed to move the systems of the master to the slave. In recent years, several controllers have been utilized to synchronize hyper–chaotic systems. Since time plays a key role in the transmission of information, ensuring a transmission with the fastest time possible is crucial. Among existing methods, the sliding–mode control (SMC) has special features such as: robustness to parametric uncertainties, simple implementation, suitable transient response, reduced order of the system, reduced sensitivity to bounded disturbances and computational simplicity.

Over several years much research has been devoted to the development and application of SMC design. Although SMC is very popular and efficient, this method suffers from a major drawback; the chattering phenomena. In practice, chattering is a very undesirable phenomenon because it can increase energy consumption, cause mechanical wear in systems and actuators and deteriorate controller performance. Hence, in designing the controller we will have two objectives, eliminating the chattering phenomena and controlling the function as quickly as possible. A lot of research has been done to solve these problems. For instance, a new chattering–free sliding mode control technique with both–differential and integral operators was proposed Li et al. for the synchronization and control of nonlinear perturbed systems with unknown parameters. A new PID sliding mode control was synthesized Mobayen to eliminate the chattering phenomena and achieve high accuracy in the presence of system disturbances.

In recent years, we have witnessed the emergence of new powerful controllers with the ability to limit time and eliminate deleterious effects on the system. The new controllers were developed for the secure communication of two various chaotic systems with unknown parameters, external disturbances and systemic uncertainty, by combining adaptive back–stepping in a finite–time and terminal sliding mode control (TSMC). Compared with the traditional sliding-mode control, the TSMC introduces a nonlinear term in the sliding surface function to improve the system’s convergence characteristics, to ensure the convergence of the system states to a given trajectory in finite time. Thus, among the advantages of TSMC are
its fast dynamic response, finite-time convergence, and high steady-state tracking accuracy.\textsuperscript{47} However, some engineering problems are expected to reach synchronization within a finite-time. The finite-time synchronization has many advantages, such as optimality of the convergence time, disturbance rejection properties and improved robustness. Generally, the synchronization refers to the tendency of the states of all coupled dynamical systems to converge to a common behavior as time evolves.

Decoding for an unauthorized receiver without knowing the initial conditions and dynamics of a hard-working system is difficult. One way to increase security in chaos communications and image transmission, is by using high-order dimensional dynamics. This is due to the fact that high-order dynamic regeneration and discovery of messages for unauthorized recipients using difficult timescale reduction methods are difficult.\textsuperscript{48–50} Other ways to enhance security in chaotic secure communications include pointing out the complexity of the system’s dynamics, because the more complex the structure of the system and the higher the number of its more parameters, the more difficult the decoding of the system. The design of high-order chaotic and hyper-chaotic systems as well as the analysis of their intrinsic properties and the stability analysis of these systems constitute some of the studies that have been conducted in this field.\textsuperscript{17–20}

Images are one of the most important carriers of information that are abundantly stored and distributed in various structures. Because most networks are open, image encryption can be an effective method. Using hyper-chaotic systems to encrypt images can increase network security and make decryption difficult.\textsuperscript{51,52} There are many ways to encrypt an image, such as: Advanced Encryption Standard,\textsuperscript{53} Data Encryption Standard\textsuperscript{54} and International Data Encryption Algorithm.\textsuperscript{55} Due to the large size of the images and the strong correlation in the images, these methods usually will not be effective.\textsuperscript{56,57} Almost all of the chaotic and hyper-chaotic image encryption algorithms, are based on changes in the values and position of the pixels.\textsuperscript{58–61}

Nowadays, DNA computing has permeated the domain of cryptography. DNA cryptogram utilizes DNA as information carrier and takes advantage of biological technology to achieve encryption.\textsuperscript{62,63} Kang et al. had proposed a character encryption algorithm based on pseudo DNA operation,\textsuperscript{64} it made use of central dogma which belongs to molecular biology to implement encryption. Wang et al.\textsuperscript{65} introduces a new DNA-based hyper-chaotic encryption algorithm that has features such as high sensitivity, large key space, and resist differential attacks. The proposed algorithm was able to reduce the time complexity and the space complexity of the permutation while achieving good permutation effects. However, DNA encryption methods have disadvantages such as expensive experimental equipment, complex operation and difficult to grasp its biotechnology, and still cannot be efficiently applied in encryption field.\textsuperscript{66,67} To overcome the disadvantages of this method, RGB encoding\textsuperscript{68,69} based on DNA encryption can be used. In this method, DNA encoding is first performed to encrypt RGB. Then three images are received after
decryption. Finally, RGB components that use Logistic chaotic images recover images. The main contributions of this paper are as follows:

- Proposing a novel exponential four-dimensional hyper-chaotic system and analyzing its inherent properties.
- Designing a new FTSMC-based controller for the fast synchronization of two different exponential hyper-chaotic systems.
- Performing color image encryption using the novel exponential hyper-chaotic system.

The remainder of the paper is organized as follows. Section 2 provides the dynamical model of the high-complexity hyper-chaotic system, displays its features and formulates the finite-time synchronization problem. Section 3 presents the design and proof of the terminal sliding-mode controller for finite-time synchronization. Section 4 discusses the implementation of the proposed chaotic system to images’ cryptosystem. In section 5, synchronization and image encryption issues are discussed using the new high-complexity hyper-chaotic system and a numerical simulation is performed to validate the methods. Some concluding remarks are finally provided in section 6.

**Problem description and preliminaries**

*Model of the hyper-chaotic system*

The dynamics of the new four-dimensional system is described as:

\[
\begin{align*}
\dot{x}_1(t) &= a_1(x_2 - x_1) - a_2x_4 - a_3x_3^2 - a_4x_2x_3 + a_3\sec h(x_1 + x_2 + x_3 + x_4) \\
\dot{x}_2(t) &= a_2x_2 + a_3x_4 - kx^2 - a_5x_2x_3 - a_2x_1x_2 - x_1x_2x_3 - a_4e^{x_3} \\
\dot{x}_3(t) &= -a_2x_3 + kx_1^2 + x_1x_2x_3 - a_1e^{x_1 + x_2 + x_4} + a_3\text{sign}(x_1 + x_2 + x_3 + x_4) \\
\dot{x}_4(t) &= -a_5x_1 + a_4x_3 + a_1x_1x_2x_3 + a_4x_2x_3x_4 + a_1x_1x_3x_4 + a_1|x_1 + x_2 + x_3 + x_4|
\end{align*}
\]

where \(x_i, (i = 1, \ldots, 4)\) and \(a_i, (i = 1, \ldots, 5)\), \(k\) are the state variables and constant positive parameters, of the system (1), respectively. With parameters (2), system (1) exhibits hyper-chaotic behaviors.

\[
a_1 = 16, a_2 = 3.85, a_3 = 20, a_4 = 8.5, a_5 = 10, k = 9. \tag{2}
\]

**Basic properties and dynamic behaviors of the hyper-chaotic system**

This section presents the natural properties of the new exponential hyper-chaotic system such as chaotic attractor’s, equilibrium point’s, Kaplan–Yorke dimension, Eigen values, Lyapunov exponents, Poincare map and Bifurcation diagram.
Analysis of equilibrium points and eigenvalues

By setting the differential equations in (1) to zero, the equilibrium points are equal to:

\[ Q^* = \left( \frac{-16}{2}, \frac{-21}{2}, \frac{-22}{2} \right) \]

When the parameter values are considered as in (1), the system linearization matrix at the equilibrium points are given by

\[
J = \left. \frac{\partial F_i}{\partial x_j} \right|_{Q^*} = \begin{bmatrix}
-16 & -21 & -22 & -4 \\
155 & -36 & 49820 & 0 \\
-106 & -22 & -16 & -20 \\
-118310 & -50 & -698 & 0
\end{bmatrix}
\]

According to (3), the system eigenvalues are found as follows:

\[
p(s) = |sI_d - J| = 0 \begin{array}{cc}
1 & 0 \\
0 & 1
\end{array}
\]

That is, \[s^4 + A_4 s^3 + A_3 s^2 + A_3 s + A_4\]

According to equation (4), the eigenvalues are \[s_1 = -707, s_2 = -146, s_{3,4} = 43 \pm 46j\]. Thus, the origin is an unstable saddle.

Chaotic attractors analysis

In hyper–chaotic systems, the phase portraits of the system start from one point and fluctuate within a certain range. Figures 1 and 2 depict the phase portrait diagrams of system (1) in 2–D and 3–D modes.
According to Figures 1 and 2, the system’s trajectories oscillate around their modes and the signal has a quasi–random behavior.

**Lyapunov exponents and Kaplan-York**

The divergence and convergence of the states of a nonlinear system, are determined by its LES representation. If LEs are positive, it indicates the chaotic behavior of the system.\textsuperscript{72,73} A system is hyper–chaotic if there are two or more positive LEs. The LEs using Wolf et al.\textsuperscript{72} method of the exponential hyper–chaotic system (1) with different initial conditions \(x_{10}(\tau) = 3.85\), \(x_{20}(\tau) = -47.26\), \(x_{30}(\tau) = 2.92\), \(x_{40}(\tau) = 2\) are numerically found as \(LE_1 = 0.192\), \(LE_2 = 0.155\), \(LE_3 = 0\), \(LE_4 = -1.163\) shown in Figures 3 and 4. Figure 5 displays the Lyapunov exponents diagram with \(k\) changes. For these values of Lyapunov exponents, the Kaplan–Yorke dimension\textsuperscript{74} of the 4D hyper–chaotic designed system, is defined as:

\[
D_{KY} = t + \frac{\sum_{i=1}^{4} LE_i}{|LE_i + 1|} = 3 + \frac{0.192 + 0.155 + 0}{|-1.163|} = 3.298
\]

which is fractional.

Table 1 numerically compares the maximum Kaplan–Yorke dimensions with a number of similar complex 4D hyper–chaotic systems (systems that have the following functions: exponential, logarithmic, trigonometric, and hyperbolic) and System (1) to determine the best system performance.
According to the results depicted in Table 1, the Kaplan–Yorke dimensions of the exponential hyper–chaotic system (1), are larger than similar systems.

Bifurcation diagram analysis

To investigate the dependence of the parameters of the new exponential hyper–chaotic system (1), we need to draw and analyze the bifurcation diagram. In Figures 6 and 7, bifurcation diagram’s of the system (1) is plotted. The system enters into chaotic oscillations with routine period doubling. Bifurcation diagrams

Figure 3. Dynamics of LEs of the novel hyper-chaotic system (1).

Figure 4. LEs spectrum of the system (1) in: (a) LE1, LE2 and (b) LE3, LE4.

According to the results depicted in Table 1, the Kaplan–Yorke dimensions of the exponential hyper–chaotic system (1), are larger than similar systems.
display the behavior of a system with respect to changes in the system parameter and explains the system’s absorbent behavior.\cite{83,84}

**Poincare map analysis**

As an interesting method, we used the Poincare map to describe the folding attributes of the chaotic system. To study the performance and behavior of continuous dynamical systems, similar to the designed system (1), we can use the Poincare map, one of the common and popular topics in nonlinear dynamic analysis. Figure 8(a) and (b) display the Poincare maps of system (1). According to Figure 8(a) and (b) the regular set of points depicted in the Poincare maps is an indication of the system’s chaotic behavior.

### Table 1. The maximum Kaplan–Yorke of similar complex hyper–chaotic systems.

| system       | LE1  | LE2  | LE3   | LE4  | $D_{KY}$ |
|--------------|------|------|-------|------|----------|
| System (1)\cite{75} | 13.463 | 3.478 | 0     | -61.231 | 3.2786   |
| System (2)\cite{76} | 0.157 | 0    | -0.245 | -0.913 | 2.6408   |
| System (3)\cite{77} | 0.064 | 0.033 | 0     | -1.25  | 3.089    |
| System (4)\cite{78} | 0.1515 | 0.0112 | 0     | -1.6623 | 3.0979   |
| System (5)\cite{79} | 0.132 | 0.035 | 0     | -1.25  | 3.13     |
| System (6)\cite{80} | 0.1555 | 0.0330 | 0     | -1.6100 | 3.1171   |
| System (7)\cite{81} | 0.1906 | 0.0450 | 0.0002 | -1.5248 | 3.1545   |
| System (8)\cite{82} | 0.1485 | 0.0392 | 0     | -1.338 | 3.1402   |
| This paper   | 0.192 | 0.155 | 0     | -1.163 | 3.298    |
One of the effective parameters in system (1) is parameter \(k\). Figure 9 displays the bifurcation diagram in system (1) with respect to the change in parameter \(k\). Figure 10 displays a 2-D diagram of the system according to its bifurcation diagram. In this figure, the \(x_1 - x_3\) graph is plotted with three different values of the initial conditions and four different \(k\) values. As it turns out, system attractors in Figure 10(c) are closer to their equilibrium points than Figure 10(a).

We can conclude from Figures 9 and 10, that the more the system becomes more chaotic, the more its attractors converge to their equilibrium points. Also, Figure...
11 displays 1–D and 3–D behaviors, and Figure 12 shows the Poincare map and 2–D behaviors of the hyper–chaotic system with changes in the $k$ parameter. Hence, by increasing the value of the parameter from $k = 7$ to $k = 10$ (see Figure 9), the system fluctuates (see Figure 10) and its complexities increase (see Figure 11).

**Problem formulation of finite–time fast synchronization**

In this section, synchronization and its theorems are presented between two new and overly hyper–chaotic systems with indefinite parameter’s and uncertain
disturbance’s. At this point, we use the system represented by equation (1) and modify the initial conditions and parameters for both the master–slave systems for fast synchronization. Consider the hyper–chaotic system that refers to the master system

\[
\dot{x}_{im}(\tau) = \begin{bmatrix}
-a_{1m} & a_{1m} - a_{4m}x_{3m} & -a_{3m}x_{3m} & -a_{2m} \\
-kx_{1m} - a_{2m}x_{2m} & -x_{1m}x_{3m} + a_{2m} & -a_{5m}x_{2m} & a_{3m} \\
kx_{1m} & x_{1m}x_{3m} & -a_{2m} & 0 \\
-a_{5m} & a_{4m}x_{3m}x_{4m} & a_{4m} + a_{1m}x_{1m}x_{2m} & a_{1m}x_{1m}x_{3m} \\
\end{bmatrix} x_{im} + \begin{bmatrix}
a_{3m}sech(x_{1m} + x_{2m} + x_{3m} + x_{4m}) \\
-a_{4m}e^{x_{3m}} \\
a_{1m}e^{(x_{1m} + x_{2m} + x_{4m})} + \text{sign}(x_{1m} + x_{2m} + x_{3m} + x_{4m}) \\
a_{1m} |(x_{1m} + x_{2m} + x_{3m} + x_{4m})| \\
\end{bmatrix}
\text{for } i = 1, \ldots, 4
\]

(6)

The basic parameters and initial conditions of the master system (6) are defined as follows:

\[
a_{1m} = 16, a_{2m} = 3.85, a_{3m} = 20, a_{4m} = 8.5, a_{5m} = 10, k = 9,
\]

\[
x_{1m}(0) = 3.85, x_{2m}(0) = -47.26, x_{3m}(0) = 2.92, x_{4m}(0) = 18.37
\]

(7)
where $X_m = x_{1m}, \ldots, x_{4m}, x_{1m}(0), \ldots, x_{4m}(0)$ and $a_{1m}, \ldots, a_{5m}$ are the states, initial conditions and parameters, of the system (6), respectively. Similarly, for the slave hyper–chaotic system we will have

\begin{figure}[h]
\centering
\includegraphics[width=\textwidth]{figure11.png}
\caption{Phase portrait trajectories (up panel) and time series (down panel) showing routes in the System (1) for varying $k$: (a) $k = 7$, (b) $k = 8$, (c) $k = 9$, and (d) $k = 10$.}
\end{figure}

\begin{figure}[h]
\centering
\includegraphics[width=\textwidth]{figure12.png}
\caption{2–D trajectories (up panel) and Poincare map (down panel) showing routes in the System (1) for varying $k$: (a) $k = 7$, (b) $k = 8$, (c) $k = 9$, and (d) $k = 10$.}
\end{figure}
where \( X_i = x_{1i}, ..., x_{5i} \) are the state variables of system (8) and \( v(\tau) = v_1, ..., v_5 \) are the nonlinear command signals used to synchronize two systems in equation (6) with equation (8). The basic parameters and initial conditions of the master system (8) are defined as follows:

\[
\begin{align*}
a_{1s} &= 25.25, a_{2s} = 4, a_{3s} = 21.27, a_{4s} = 9, a_{5s} = 11.5, k = 10, \\
x_{1s}(0) &= 5, x_{2s}(0) = -62, x_{3s}(0) = 4.25, x_{4s}(0) = 20
\end{align*}
\]  

(9)

where \( x_{1i}(0), ..., x_{4i}(0) \) and \( a_{1s}, ..., a_{5s} \) are the initial conditions and parameters of slave System (6), respectively.

**Assumption 1.** Let the synchronization and fast synchronization errors of System (6) and System (8) be as: \( e_i = x_{is} - x_{im}(i = 1, ..., 4) \).

**Assumption 2.** In general, consider the constraints on the disturbance and uncertainty as:

\[
|f(x(\tau))| \leq \alpha_1, |d(\tau)| \leq \alpha_2
\]  

(10)

where \( \alpha_1 \) and \( \alpha_2 \) denote positive unknown constants.

**Assumption 3.** Suppose \( y_i(\tau) = x_i(\tau) \) implies that \( \lim_{\tau \to \infty} e_i(\tau) = 0 \).

**Definition 1.** Systems (6) and (8) can be synchronized in a finite-time if \( \lim_{\tau \to T} ||error(\tau)|| = 0 \) and \( ||error(\tau)|| = 0 \) if \( \tau \geq T \), where \( T = T(error(0)) > 0 \), 

\[
error(\tau) = [error]_T, (i = 1, ..., 4).
\]

**Definition 2.** Master–slave systems (6) and (8) are finite–time synchronized, if there is a controller \( v_p(\tau) \) and a constant \( T > 0 \) such that \( \lim_{\tau \to T} [Z^*_p(\tau) - Z'^*_p(\tau)] = 0 \), where \( Z^*_p(\tau) - Z'^*_p(\tau) \) for \( \tau > T \), \( Z^*(\tau) \) and \( Z'^*(\tau) \) are the solutions of master–slave Systems (6) and (8).

**Lemma 1.** If the \( \theta(\tau) \) is a definite and positive performance such that:

\[
\dot{\theta}(\tau) \leq -\psi \theta^\theta(\tau), \forall \tau \geq \tau_0, \theta(\tau_0) \geq 0
\]  

(11)
where $\psi > 0, 0 < \theta < 1$ are known and constants, for any initial time $\tau_0$. Then function $\vartheta(t)$ satisfies

$$
\vartheta^{1-\theta}(\tau) \leq \vartheta^{1-\theta}(\tau_0) - \psi(1 - \theta)(\tau - \tau_0), \tau_0 \leq \tau \leq \tau_1
$$

(12)

and

$$
\vartheta(\tau) \equiv 0, \forall \tau \geq \tau_1
$$

(13)

with the settling time $\tau_1$ satisfying

$$
\tau_1 \leq \tau_0 + \frac{\vartheta^{1-\theta}(\tau_0)}{\psi(1 - \theta)}
$$

(14)

**Lemma 2.** Suppose that the $\nu(\tau)$ function, which is positive–definite and continuous, satisfies the differential inequality of [25]:

$$
\dot{\nu}(\tau) \leq -\alpha \nu(\tau) - \beta \nu^{\eta}(\tau) \forall \tau \geq \tau_0, \nu(\tau_0) \geq 0
$$

(15)

for all times $\tau_0$, the function $\nu(\tau)$ in the finite time $\tau_s$, will converge to zero. Thus:

$$
\tau_s = \tau_0 + \frac{1}{\alpha(1 - \eta)} \ln \frac{\alpha \nu^{1-\eta}(\tau_0) + \beta}{\beta}
$$

(16)

**Main results of fast synchronization**

Consider the dynamical model as:

$$
\dot{x}(\tau) = Ax(\tau) + B\nu(\tau) + f(x(\tau)) + d(\tau),
$$

(17)

where $x(\tau)$ is the system state variable, $A$ and $B$ are the constant matrices, $\nu(\tau)$ is the controller, $f(x(\tau))$ is the nonlinear functions of the system and $d(\tau)$ is the uncertain disturbance of the system. The sliding surface for the system (17) is described as:

$$
l(\tau) = Gx(\tau)
$$

(18)

where $G$ is the gain coefficient (row vector) as $G = [\varphi_1, \varphi_2, \varphi_3, \varphi_4, \varphi_5]$.

In order to satisfy $l(\tau)$ converges to origin in the finite–time, the following fast terminal sliding surface is given as:

$$
s(\tau) = l(\tau) + \lambda l(\tau) + \mu l^{\eta}(\tau),
$$

(19)

where $\lambda$ and $\mu$ signify the positive constant values of the system, and $\eta$ is a ratio of two odd positive integers with $1 > \eta > 0$.

**Theorem 1.** Consider the disturbed dynamic system (17). Let the fast terminal sliding controller be defined as:
\[ \dot{v}(\tau) = -(GB)^{-1} \{ (\lambda + \mu \eta(t)^{n-1}) G[Ax(\tau) + Bu(\tau) + f(x(\tau))] \\
+ G(\Lambda^2 x(\tau) + \Lambda Bu(\tau) + Af(x(\tau)) + \dot{f}(x(\tau))) + \kappa|s(\tau)|^n + \gamma s(\tau) + \chi \operatorname{sgn}(s(\tau)) \}, \]

where \( \gamma \) and \( \kappa \) are optional positive constants and \( \chi \) is a scalar value which satisfies

\[ \chi \geq \max \left[ \left( (\lambda + \mu \eta(t)^{n-1}) G + \Lambda G \right) d(\tau) + G \dot{d}(\tau) \right]. \]

Then, the states of the dynamical system (17) move to the sliding surface (18) in finite-time and remain on it.

**Proof.** The Lyapunov candidate function can be considered as follows:

\[ V(\tau) = 0.5s(\tau)^2 \]  

From (19), the time-derivative of the fast terminal sliding surface is found as:

\[ \dot{s}(\tau) = \ddot{l}(\tau) + (\lambda + \mu \eta(t)^{n-1}) \dot{l}(\tau), \]

where using (17) and (18), we have:

\[ \dot{s}(\tau) = G\ddot{x}(\tau) + (\lambda + \mu \eta(t)^{n-1}) G\dot{x}(\tau) \\
= G(\Lambda \ddot{x}(\tau) + B\dot{u}(\tau) + \dot{f}(x(\tau)) + \dot{d}(\tau)) + (\lambda + \mu \eta(t)^{n-1}) G\dot{x}(\tau) \\
= G(\Lambda^2 x(\tau) + \Lambda Bu(\tau) + Af(x(\tau)) + \Lambda d(\tau) + B\dot{u}(\tau) + \dot{f}(x(\tau)) + \dot{d}(\tau)) \\
+ (\lambda + \mu \eta(t)^{n-1}) G[Ax(\tau) + Bu(\tau) + f(x(\tau)) + d(\tau)]. \]

Differentiating the Lyapunov function (22) and using (24) yields:

\[ \ddot{V}(\tau) = s(\tau) \{ (\lambda + \mu \eta(t)^{n-1}) G[Ax(\tau) + Bu(\tau) + f(x(\tau)) + d(\tau)] \\
+ G(\Lambda^2 x(\tau) + \Lambda Bu(\tau) + Af(x(\tau)) + \Lambda d(\tau) + B\dot{u}(\tau) + \dot{f}(x(\tau)) + \dot{d}(\tau)) \}, \]

where substituting (20) into (25), yields:

\[ \ddot{V}(\tau) = -\kappa|s(\tau)|^{n+1} - \gamma s(\tau)^2 - \chi s(\tau) \operatorname{sgn}(s(\tau)) + s(\tau) \left( (\lambda + \mu \eta(t)^{n-1}) G + \Lambda G \right) d(\tau) + G \dot{d}(\tau) \]

\[ \leq -\kappa|s(\tau)|^{n+1} - \gamma s(\tau)^2 - \chi |s(\tau)| + |s(\tau)| \left( (\lambda + \mu \eta(t)^{n-1}) G + \Lambda G \right) d(\tau) + G \dot{d}(\tau) | \]

Using (21) and (26), we can write:

\[ \ddot{V}(\tau) \leq -\gamma|s(\tau)|^2 - \kappa|s(\tau)|^{n+1} = -\alpha V(\tau) - \beta \dot{V}(\tau) \]
where $\bar{\eta} = (\eta + 1)/2 < 1$, $\alpha = 2\gamma > 0$ and $\beta = 2^\eta \kappa > 0$. This means that the Lyapunov function (22) is decreased gradually and the sliding surface converges to the origin in finite–time. Consequently, this completes the proof.

### Application in images’ cryptosystem

In this section, the proposed 4D hyper–chaotic system (1) is implemented to an image cryptosystem. Without loss of generality, an 8–bit RGB color image of size $M \times M$ is used as an original image. The encryption and decryption procedures are explained below.

#### Image encryption and decryption

One of the newest and most successful methods of chaos encryption is DNA–based encryption. The development of DNA encryption is due to the advancement of DNA computing. In genetics, each DNA contains four basic types: Cytosine–Guanine–Adenine–Thymine (C–G–A–T). According to the DNA algorithm, the coding corresponds to four nucleus (A–G–C–T) bases using four digits (0,0), (0,1), (1,0), (1,1). So, there are $4!$ coding patterns with this method, which are shown in

---

**Table 2.** DNA encryption and decryption algorithm.

|   | 1   | 2   | 3   | 4   | 5   | 6   | 7   | 8   |
|---|-----|-----|-----|-----|-----|-----|-----|-----|
| A | (0–0)| (0–0)| (0–1)| (0–1)| (1–0)| (1–0)| (1–0)| (1–0) |
| T | (1–1)| (1–1)| (1–0)| (1–0)| (0–1)| (0–1)| (0–0)| (0–0) |
| G | (0–1)| (1–0)| (0–0)| (1–1)| (0–0)| (1–1)| (0–1)| (1–0) |
| C | (1–0)| (0–1)| (1–1)| (0–0)| (1–1)| (0–0)| (1–0)| (0–1) |

---

**Figure 13.** DNA color image encryption flowchart using hyper–chaotic system (1).
Table 2. Figure 13 shows the flowchart of DNA color image encryption using the exponential hyper–chaotic system (1).

Details on the encryption and decryption process are described as follows:

(1) The digital image is divided into three two–dimensional matrices according to equation (28).

\[
\begin{align*}
I_1 &= I(:, :, 1) \\
I_2 &= I(:, :, 2) \\
I_3 &= I(:, :, 3)
\end{align*}
\] (28)

(2) Dividing RGB into sub–matrices and converting the analyzed matrices into binary matrices under:

\[
\begin{align*}
R(m, n\times j) \\
G(m, n\times j) &= 8 \\
B(m, n\times j)
\end{align*}
\] (29)

(3) Create \(x_n\) with length \(l = m\times n\times 8/2\) with chaotic logistics function (30) and with initial conditions and parameter \(x_0, \mu_0\).

\[
x_n = \mu x_{n-1}(1 - x_{n-1})
\] (30)

(4) Set the trail length on \(M\times N_0\), appropriate value setting of parameter \(\mu\) as password and selection of initial conditions of \(x_0\) as follows:

\[
x_0 = \frac{\text{sum}(I_1, :) + \text{sum}(I_2, :)}{\text{sum}(I_1, :) + \text{sum}(I_2, :)} \times \frac{2\times M\times N}{2\times M\times N \times 255}
\] (31)

where, \(\text{sum}(I_1, :)\), \(\text{sum}(I_2, :)\) is a set of \(R, G\) channel positions that need to be encrypted. The \(x_0\) is the key to the password as well as the average \(I_1, I_2\).

(5) Convert \(x_i, y_i\) sequence values to numbers \(1, ..., 8\) according to:

\[
\begin{align*}
x &= \text{mod}(\text{round}(x\times10^4), 8) + 1 \\
y &= \text{mod}(\text{round}(y\times10^4), 8) + 1
\end{align*}
\] (32)

where the value of \(x_i\) is a random number in the range \(x_i \in (1, 8)\).
Since 4 algorithms are used for DNA, the $z_i$ sequence is determined between 0, ..., 3 and the following equation:

$$z = \text{mod}(\text{round}(x \times 10^4), 4)$$  \hspace{1cm} (33)

where the $z_i$ sequence is determined by the hyper–chaotic system (1).

The original image can be recovered by applying a reverse operation in the encryption process.

**Simulation results**

**Simulation results of fast synchronization**

In this section, we perform a fast synchronization between two four–dimensional hyper–chaotic systems with unknown disturbances and parametric uncertainty to the system. Here, we used both the System (6) and System (8) for the synchronization. Figure 14 display the amazing hyper–chaotic attractors of the master (6) and slave (8) systems with initial conditions and parameters (7) and (9).

According to Assumption 2, disturbances have been applied to the slave system (8). It is worth noting that although the systems (6) and (8) are the same, for their simulation during synchronization, we considered unequal parameters and different initial conditions. According to Figure 14, all the modes of the master–slave systems behave differently. Based on Assumption 1, to study chaos synchronization, the error according to systems (6) and (8), can be computed as follows:
\[ e_i = \sum_{i=1}^{4} y_i - x_i \]

\[
\begin{bmatrix}
\dot{e}_1 \\
\dot{e}_2 \\
\dot{e}_3 \\
\dot{e}_4
\end{bmatrix} = 
\begin{bmatrix}
-a_1 e_1 + a_1 e_2 - a_2 e_4 + f_1(\tau) \\
-a_2 e_2 + a_3 e_4 + f_2(\tau) \\
-a_3 e_3 + f_3(\tau) \\
-a_4 e_1 + a_4 e_3 + f_4(\tau)
\end{bmatrix} + B(\tau)u(\tau) + D(\tau)
\]

\[ (34) \]

where

\[
f_1(\tau) = a_{3m}x_{3m}^2 + a_{4m}x_{2m}x_{3m} - a_{3s}x_{3s}^2 - a_{4s}x_{2s}x_{3s} \]

\[
f_2(\tau) = kx_{1m}^2 + a_{5m}x_{2m}x_{3m} + a_{2m}x_{1m}x_{2m} + x_{1m}x_{2m}x_{3m} + a_{4m}e^{-x_{3m}}
- kx_{1s}^2 - a_{5s}x_{2s}x_{3s} - a_{2s}x_{1s}x_{2s} - x_{1s}x_{2s}x_{3s} - a_{4s}e^{x_{3s}}
\]

\[
f_3(\tau) = -kx_{1m}^2 - x_{1m}x_{2m}x_{3m} + a_{1m}e^{-(x_{1m} + x_{2m} + x_{3m})} - a_{3m}m\text{sign}(x_{1m} + x_{2m} + x_{3m} + x_{4m})
+ kx_{1s}^2 + x_{1s}x_{2s}x_{3s} - a_{1s}e^{(x_{1s} + x_{2s} + x_{3s})} + a_{3s}m\text{sign}(x_{1s} + x_{2s} + x_{3s} + x_{4s})
\]

\[
f_4(\tau) = -a_{1m}x_{1m}x_{2m}x_{3m} - a_{4m}x_{2m}x_{3m}x_{4m} - a_{1m}x_{1m}x_{3m}x_{4m} - a_{1m}|x_{1m} + x_{2m} + x_{3m} + x_{4m}|
+ a_{1s}x_{1s}x_{2s}x_{3s} + a_{4s}x_{2s}x_{3s}x_{4s} + a_{1s}x_{1s}x_{3s}x_{4s} + a_{1s}|x_{1s} + x_{2s} + x_{3s} + x_{4s}|
\]

\[ (35) \]

The systems (34) and (35) can be represented in matrix form as follows:

\[
\frac{de_i(\tau)}{d\tau} = \Lambda e_i(\tau) + f(e(\tau)) + B(\tau)u(\tau) + D(\tau)
\]

\[ (36) \]

where

\[
e_i(\tau) = 
\begin{bmatrix}
e_1 \\
e_2 \\
e_3 \\
e_4
\end{bmatrix}, B(\tau) = 
\begin{bmatrix}1 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 \\
0 & 0 & 0 & 1
\end{bmatrix}, f(e(\tau)) = 
\begin{bmatrix}f_1(\tau) \\
f_2(\tau) \\
f_3(\tau) \\
f_4(\tau)
\end{bmatrix}
\]

\[ (37) \]

\[
\Lambda = 
\begin{bmatrix}
-a_1 a_1 - a_2 & 0 & 0 & 0 \\
0 & a_2 a_3 & 0 & 0 \\
0 & 0 & -a_3 a_4 & 0 \\
-a_5 a_4 & 0 & 0 & -a_5 a_4
\end{bmatrix}, D(\tau) = 
\begin{bmatrix}3\cos(t) \\
12\sin(6t) \\
9\cos(2t) - 0.1 \\
14\sin(4t) + 7.5
\end{bmatrix}
\]

Then, based on Theorem 1, we trust that the fast synchronization between system (6) and system (8) with error equation (36), will be achieved in finite–time. In the TSMC design, we use the controller defined in (20). According to the SMC law, gains are selected as:

\[
G = [\varphi_1 \varphi_2 \varphi_3 \varphi_4] = [5805 - 720 - 482]
\]

\[ (38) \]
The functions $d(t)$ and $f(t)$ are given in the form of (37). The sliding surface is defined according to equation (19) and considering $\lambda = 17$, $\mu = 50$, $\eta = 1/19$. The control law (20) is designed with $\kappa = 20$, $\gamma = 38$ to ensure the fast synchronization of the unknown hyper-chaotic systems. Figure 15 displays the complete hyper-chaos synchronization of system (6) and (8). According to (37), when the controller is activated, the errors of synchronization obtained are the same as those depicted in Figure 16. We will have fast synchronization when the error reaches zero in finite-time.

According to the simulation results (see Figures 15 and 16), despite the fact that we proved that the exponential hyper-chaotic system (1) has a lot of fluctuations,
the controller (20) was able to reduce the error to zero in $t = 0.319s$. Hence, it can easily be observed that the master–slave systems are synchronized in finite–time.

In what follows, to further assess the performance of the control approach, we compare its performance to the observer-based composite adaptive terminal sliding-mode approach proposed Liu et al.\textsuperscript{1} Figure 17 displays the output of the system using the controller (20) compared to the outputs of the reference model and method Liu et al.\textsuperscript{1} The time response of the tracking errors are shown in Figure 18. From Figure 18, it is demonstrated that the tracking error signal appropriately converges to the origin and provides faster tracking performance than method.\textsuperscript{1}
Results of images’ encryption

In this subsection, the usefulness of the application of the proposed scheme for image encryption is validated using numerical simulations. “Lena” image in PNG format are used in this simulation as the original data which must be encrypted (see Figure 19(a)). The encryption keys are generated by the encryptor hyper–chaotic system. By applying these chaotic keys and the encryption method described in Subsection 4.1, the original image is encrypted. Figure 19 shows the obtained encrypted image. At the decryptor, the exponential hyper–chaotic system is used to generate the decryption keys. The decrypted “Lena” image can be obtained after the synchronization procedure and the above-mentioned decryption process (see Figure 19(c)). From these figures, it can be observed that the encrypted image have a uniform distribution, and the encrypted image are similar to the noise. It is demonstrated that in terms of visual impression, the suggested method has a good encryption performance.

Performance analysis of the proposed cryptosystem

Security analysis is performed to analyze the robustness and demonstrate the efficiency of the proposed method. In order to show the efficiency of hyper–chaotic cryptography, key space analysis, histogram analysis and correlation test have been used.

Key space analysis

The key–space size for a cryptosystem is based on the total number of various keys that are utilized in the encryption. A successful cryptosystem should possess a key space which is great enough to resist all kinds of brute–force attacks. These types of attacks are actually based on the exhaustive key search. In the proposed algorithm, if the eavesdroppers want to extract the original satellite image from the encrypted image, they will require the system initial conditions and the parameters...
of the hyper–chaotic system (equations (3) and (4)) as secret keys. All of these
secret keys are considered as type double, which has 15-digit accuracy. Therefore,
the key space becomes as huge as $(10^{14})^{16} = 10^{224} \approx 2^{774}$. Thus, it can be claimed
that the proposed algorithm possesses a large key–space which is capable of resist-
ing all possible kinds of statistical attacks.

**Histogram analysis**

To barricade the revelation of image information by an eavesdropper, it is useful if
the encrypted image has no or very few statistical similarities to the original image.
The distribution of pixel elements in an image with the color intensity of each pixel
element is displayed by the image histogram. Histogram analysis is performed to
detect the distribution of pixel values and uniform coding. Once this chart is uni-
form, we will have secure encryption. Figure 20 illustrates the histograms of the
red–green–blue color channels of the original and encrypted images of the “Lena.”

As shown in Figure 20(d–f), the dissemination of the pixels is evenly distributed,
so no information about the original image can be obtained from Figure 19.

**Correlation test**

Another indicator in statistical analysis is the use of adjacent pixel correlation,
which includes vertical–horizontal–diagonal correlation. The degree of image resis-
tance to attack is proportional to the correlation of the location data adjacent to
the pixels. Figure 21 demonstrates the correlation between the pixels in the ‘Lena’ shape. In this figure, 5000 pixel points are used.

According to Figure 21, the values of vertical–horizontal–diagonal correlation are approximately close to one, indicating a high–correlation between pixels. The correlation values of the encrypted image are close to zero, and this indicates that the values of vertical–horizontal–diagonal correlation of the channels have nothing to do with each other. Table 3 compares the vertical–horizontal–diagonal correlation of the Lena image.

The correlation data of the pixels adjacent to Lena’s image in Table 3 after encryption in three directions are very small and this proves that the image is encrypted with a higher degree of confusion.

![Figure 21. Correlation between pixels of “monkey” image for: (a–c) original image and (d–f) encrypted image.](image)

| Images                          | Horizontal | Vertical | Diagonal |
|--------------------------------|------------|----------|----------|
| Original Lena image for all     | 0.9491     | 0.9673   | 0.946    |
| Encryption Lena image in Tian and Lu$^{90}$ | −0.0020     | −0.0015  | −0.0012  |
| Encryption Lena image in Elamrawy et al.$^{91}$ | 0.0015      | −0.0037  | 0.0079   |
| Encryption Lena image in Sun$^{92}$ | 0.0013      | 0.0021   | −0.0024  |
| Encryption Lena image in Stalin et al.$^{93}$ | 0.0052      | 0.0031   | 0.0019   |
| Encrypted Lena image in this paper | 0.0014     | −0.0016  | −0.0011  |

Table 3. Comparison between horizontal–vertical–diagonal correlation coefficient of Lena image.
IE, NPCR, and UACI metrics

At last, in this subsection, the other useful metrics for image cryptosystem quality measurement such as IE, UACI, and NPCR are computed. In information entropy theory, the complexity of encrypted data is specified. We can determine complexity of the encrypted data with information entropy theory. The information entropy for an image is calculated as

\[
IE(f) = \sum_{i=1}^{255} h(\phi_i) \log \left( \frac{1}{h(\phi_i)} \right)
\]

where \( h(\phi_i) \) demonstrates the probability of variable \( \phi_i \) and the entropy is calculated in bits. The information entropy value for a truly random source is equal to 8. The closer the information entropy get to 8, the quality of the encryption is going better. IE value of the suggested encryption technique is equal to 7.9846. It seems that IE value of the advised scheme is very close to 8.

Moreover, to measure the robustness of the encryption process in differential attacks, the NPCR and UACI values are considered. In fact, the rate of change in the result of encryption process when the difference between the original images is very small can be measured by the NPCR and UACI quantities. Suppose that \( CI_1 \) and \( CI_2 \) are two encrypted images after and before changing one pixel of the original image at the position \( i, j \), and \( \lambda(i,j) \) is a bipolar array defined as

\[
\lambda(i,j) = \begin{cases} 
1 & \text{if} \ CI_1(i,j) \neq CI_2(i,j) \\
0 & \text{if} \ CI_1(i,j) = CI_2(i,j)
\end{cases}
\]

Now, the NPCR and UACI quantities are calculated as

\[
NPCR(CI_1, CI_2) = \frac{\sum_{i,j} \lambda(i,j)}{S} \times 100\% \tag{41}
\]

\[
UACI(CI_1, CI_2) = \frac{\sum_{i,j} |CI_1(i,j) - CI_2(i,j)|}{SF} \times 100\% \tag{42}
\]

where \( S \) represents the total number of pixels in the original image and \( F \) is the value of the largest theoretical allowed value in the encrypted image. The optimal values of NPCR and UACI are \( NPCR_{opt} = 99.61\% \) and \( UACI_{opt} = 33.46\% \), respectively. The values of NPCR and UACI of the suggested encryption method are 99.53\% and 33.39\%, respectively. Note that the NPCR and UACI values are very close to the optimal values. It can then be concluded based on the practical results and performance analysis that the suggested cryptosystem is able to perfectly hide the information of the image.

Remark 1. In real scenarios, transmission channel adds the noise \( n_d(t) \) to the encrypted signal. To clean the encrypted signals from the noise, a bank of filters can be considered as the butterworth type at the input of the receiver.\textsuperscript{96,97}
Conclusions

This paper proposed a novel exponential 4D hyper–chaotic system with extremely complicated dynamics and structure. It also analyzed the dynamic behaviors of the proposed using phase portraits, Lyapunov exponent, Poincare map, Kaplan–Yorke dimension and bifurcation diagram. Then it proposed a terminal sliding mode controller to stabilize the new hyper–chaotic system with uncertainty and unknown disturbances. Stability analysis was established using the Lyapunov stability theory. The controller is designed to ensure the fast synchronization between two similar proposed hyper–chaotic systems in the presence of unequal parameters, different initial conditions and matched disturbances for transfer industrial automation information. The approach was implemented for images cryptosystem. Color image encryption was also carried out to confirm the performance of the new hyper–chaotic system. For image encryption, the DNA encryption-based RGB algorithm was used. Performance assessment of the proposed approach confirmed the ability of the proposed hyper–chaotic system to increase the security of image encryption.

Declaration of conflicting interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author(s) received no financial support for the research, authorship, and/or publication of this article.

ORCID iD

Javad Mostafaee https://orcid.org/0000-0002-6114-3051

References

1. Liu X, Qi S, Malekain R, et al. Observer-based composite adaptive dynamic terminal sliding-mode controller for nonlinear uncertain SISO systems. *Int J Control Autom Syst* 2019; 17: 94–106.
2. Bakhache B, Ahmad K and El Assad S. Chaos based improvement of the security of ZigBee and Wi-Fi networks used for industrial controls. In: *International conference on information society (i-Society 2011)*, London, UK, 27–29 June 2011, pp.139–145. New York, NY: IEEE.
3. Wollschlaeger M, Sauter T and Jasperneite J. The future of industrial communication: Automation networks in the era of the internet of things and industry 4.0. *IEEE Ind Electron Mag* 2017; 11: 17–27.
4. Pai MC. Chaos control of uncertain time-delay chaotic systems with input dead-zone nonlinearity. *Complexity* 2016; 21: 13–20.
5. Hoang TM. A Chaos-based image cryptosystem using nonstationary dynamics of logistic map. In: 2019 International conference on Information and Communication Technology Convergence (ICTC), Jeju Island, Korea, 16–18 October 2019, pp.591–596. New York, NY: IEEE.

6. Mobayen S, Vaidyanathan S, Sambas A, et al. A novel chaotic system with boomerang-shaped equilibrium, its circuit implementation and application to sound encryption. Iran J Sci Technol Trans Electr Eng 2019; 43: 1–12.

7. Tlelo-Cuautle E, Ramos-López HC, Sánchez-Sánchez M, et al. Application of a chaotic oscillator in an autonomous mobile robot. J Electr Eng 2014; 65: 157–162.

8. Minati L, Ito H, Perinelli A, et al. Connectivity influences on nonlinear dynamics in weakly-synchronized networks: insights from Rössler systems, electronic chaotic oscillators, model and biological neurons. IEEE Access 2019; 7: 174793–174821.

9. Huang Y and Yang X-S. Hyperchaos and bifurcation in a new class of four-dimensional Hopfield neural networks. Neurocomputing 2006; 69: 1787–1795.

10. Zhou A, Wang S and Wang F. Low-complexity and robust detection for hybrid chaos communication. In: 2019 11th International conference on Wireless Communications and Signal Processing (WCSP), Xi’an, China, 23–25 October 2019, pp.1–5. New York, NY: IEEE.

11. Zhang S and Gao T. A coding and substitution frame based on hyper-chaotic systems for secure communication. Nonlinear Dyn 2016; 84: 833–849.

12. Chen G and Ueta T. Yet another chaotic attractor. Int J Bifurcation Chaos 1999; 9: 1465–1466.

13. Lü J and Chen G. A new chaotic attractor coined. Int J Bifurcation Chaos 2002; 12: 659–661.

14. Qi G, Chen G, Du S, et al. Analysis of a new chaotic system. Physica A 2005; 352: 295–308.

15. Dimassi H and Loria A. Adaptive unknown-input observers-based synchronization of chaotic systems for telecommunication. IEEE Trans Circuits Syst I Regul Pap 2010; 58: 800–812.

16. Al-sawalha MM and Al-Dababseh AF. Nonlinear anti-synchronization of two hyper chaotical systems. Appl Math Sci 2011; 5: 1849–1856.

17. Kapitaniak T and Chua LO. Hyperchaotic attractors of unidirectionally-coupled Chua’s circuits. Int J Bifurcation Chaos 1994; 4: 477–482.

18. Guang-Yi W, Jing-Biao L and Xin Z. Analysis and implementation of a new hyperchaotic system. Chin Phys 2007; 16: 2278.

19. Mahmoud GM, Ahmed ME and Mahmoud EE. Analysis of hyperchaotic complex Lorenz systems. Int J Mod Phys C 2008; 19: 1477–1494.

20. Yu H, Cai G and Li Y. Dynamic analysis and control of a new hyperchaotic finance system. Nonlinear Dyn 2012; 67: 2171–2182.

21. Wang C, Xia H and Zhou L. A memristive hyperchaotic multiscroll jerk system with controllable scroll numbers. Int J Bifurcation Chaos 2017; 27: 1750091.

22. Dong E, Zhang Z, Yuan M, et al. Ultimate boundary estimation and topological horseshoe analysis on a parallel 4D hyperchaotic system with any number of attractors and its multi-scroll. Nonlinear Dyn 2019; 95: 3219–3236.

23. Tahir FR, Ali RS, Pham V-T, et al. A novel autonomous 2S\varvec{ }butterfly wig chaotic attractor. Nonlinear Dyn 2016; 85: 2665–2671.

24. Franco FF, Rempel EL and Muñoz PR. Crisis and hyperchaos in a simplified model of magnetoconvection. Physica D 2020; 406: 132417.
25. Leutcho GD, Kengne J and Kengne R. Remerging Feigenbaum trees, and multiple coexisting bifurcations in a novel hybrid diode-based hyperjerk circuit with offset boosting. *Int J Dyn Control* 2019; 7: 61–82.

26. Njitacke ZT, Kengne J and Fotsin H. Coexistence of multiple stable states and bursting oscillations in a 4D Hopfield neural network. *Circuits Syst Signal Process* 2020; 39: 3424–3444.

27. Matouk A. Dynamics and control in a novel hyperchaotic system. *Int J Dyn Control* 2019; 7: 241–255.

28. Szumniński W. Integrability analysis of chaotic and hyperchaotic finance systems. *Nonlinear Dyn* 2018; 94: 443–459.

29. Prakash P, Rajagopal K, Koyuncu I, et al. A novel simple 4-D hyperchaotic system with a saddle-point index-2 equilibrium point and multistability: design and FPGA-based applications. *Circuits Syst Signal Process* 2020; 39: 4259–4280.

30. Deng Q, Wang C and Yang L. Four-wing hidden attractors with one stable equilibrium point. *Int J Bifurcation Chaos* 2020; 30: 2050086.

31. Jalnine AY. Generalized synchronization of identical chaotic systems on the route from an independent dynamics to the complete synchrony. *Regul Chaotic Dyn* 2013; 18: 214–225.

32. Gonchenko AS, Gonchenko SV and Kazakov AO. Richness of chaotic dynamics in nonholonomic models of a Celtic stone. *Regul Chaotic Dyn* 2013; 18: 521–538.

33. Barhaghtalab MH, Mobayen S and Merrikh-Bavat F. Design of a global sliding mode controller using hyperbolic functions for nonlinear systems and application in chaotic systems. In: 2019 27th Iranian Conference on Electrical Engineering (ICEE), Yazd, Iran, 30 April–2 May 2019, pp.1030–1034. New York, NY: IEEE.

34. Wu X, Zhu C and Kan H. An improved secure communication scheme based passive synchronization of hyperchaotic complex nonlinear system. *Appl Math Comput* 2015; 252: 201–214.

35. Singh PP, Singh JP and Roy B. Tracking control and synchronization of Bhalekar-Gejji chaotic systems using active backstepping control. In: 2018 IEEE International Conference on Industrial Technology (ICIT), Lyon, France, 19–22 February 2018, pp.322–326. New York, NY: IEEE.

36. Henein MM, Sayed WS, Radwan AG, et al. Switched active control synchronization of three fractional order chaotic systems. In: 2016 13th International conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON), Chiang Mai, Thailand, 28 June–1 July 2016, pp.1–6. New York, NY: IEEE.

37. Liu Z. Design of nonlinear optimal control for chaotic synchronization of coupled stochastic neural networks via Hamilton–Jacobi–Bellman equation. *Neural Netw* 2018; 99: 166–177.

38. Mobayen S and Javadi S. Disturbance observer and finite-time tracker design of disturbed third-order nonholonomic systems using terminal sliding mode. *J Vib Control* 2017; 23: 181–189.

39. Pisano A and Usai E. Output-feedback control of an underwater vehicle prototype by higher-order sliding modes. *Automatica* 2004; 40: 1525–1531.

40. Besnard L, Shtessel YB and Landrum B. Quadrotor vehicle control via sliding mode controller driven by sliding mode disturbance observer. *J Franklin Inst* 2012; 349: 658–684.
41. Konishi K, Hirai M and Kokame H. Sliding mode control for a class of chaotic systems. *Phys Lett A* 1998; 245: 511–517.

42. Yau H-T, Chen Co-K and Chen C-L. Sliding mode control of chaotic systems with uncertainties. *Int J Bifurcation Chaos* 2000; 10: 1139–1147.

43. Li H, Liao X, Li C, et al. Chaos control and synchronization via a novel chattering free sliding mode control strategy. *Neurocomputing* 2011; 74: 3212–3222.

44. Mobayen S. An adaptive chattering-free PID sliding mode control based on dynamic sliding manifolds for a class of uncertain nonlinear systems. *Nonlinear Dyn* 2015; 82: 53–60.

45. Xi X, Mobayen S, Ren H, et al. Robust finite-time synchronization of a class of chaotic systems via adaptive global sliding mode control. *J Vib Control* 2018; 24: 3842–3854.

46. Zirkohi MM. An efficient approach for digital secure communication using adaptive backstepping fast terminal sliding mode control. *Comput Electr Eng* 2019; 76: 311–322.

47. Zak M. Terminal attractors for addressable memory in neural networks. *Phys Lett A* 1988; 133: 18–22.

48. Yang F, Mou J, Liu J, et al. Characteristic analysis of the fractional-order hyperchaotic complex system and its image encryption application. *Signal Process* 2020; 169: 107373.

49. Xu C, Sun J and Wang C. An image encryption algorithm based on random walk and hyperchaotic systems. *Int J Bifurcation Chaos* 2020; 30: 2050060.

50. Mehdi SA and Ali ZL. Image encryption algorithm based on a novel six-dimensional hyper-chaotic system. *Al-Mustansiriyah J Sci* 2020; 31: 71–75.

51. Li C, Zhao F, Liu C, et al. A hyperchaotic color image encryption algorithm and security analysis. *Secur Commun Netw* 2019; 2019: 1–8.

52. Xu J, Li P, Yang F, et al. High intensity image encryption scheme based on quantum logistic chaotic map and complex hyperchaotic system. *IEEE Access* 2019; 7: 167904–167918.

53. D’souza FJ and Panchal D. Advanced encryption standard (AES) security enhancement using hybrid approach. In: 2017 *International Conference on Computing, Communication and Automation (ICCCA)*, Galgotias University, Greater Noida, India, 5–6 May 2017, pp.647–652. Piscataway, NJ: IEEE.

54. Arboleda ER, Balaba JL and Espineli JCL. Chaotic Rivest-Shamir-Adlerman algorithm with data encryption standard scheduling. *Bull Electr Eng Inf* 2017; 6: 219–227.

55. Rahim R, Mesran M and Siahaan APU. Data security with international data encryption algorithm. 2017.

56. Abd El-Latif AA, Li L and Niu X. A new image encryption scheme based on cyclic elliptic curve and chaotic system. *Multimed Tools Appl* 2014; 70: 1559–1584.

57. Zhang X, Fan X, Wang J, et al. A chaos-based image encryption scheme using 2D rectangular transform and dependent substitution. *Multimed Tools Appl* 2016; 75: 1745–1763.

58. Li P, Xu J, Mou J, et al. Fractional-order 4D hyperchaotic memristive system and application in color image encryption. *EURASIP J Image Video Process* 2019; 2019: 22.

59. Li Z, Jiang A and Mu Y. Research on image encryption algorithm based on wavelet transform and Qi hyperchaos. In: *International conference in communications, signal processing, and systems*, Urumqi, China, 20–22 July 2019, pp.796–810. Springer.

60. Niyat AY, Moattar MH and Torshiz MN. Color image encryption based on hybrid hyper-chaotic system and cellular automata. *Opt Lasers Eng* 2017; 90: 225–237.
61. Zhou N, Chen W, Yan X, et al. Bit-level quantum color image encryption scheme with quantum cross-exchange operation and hyper-chaotic system. *Quantum Inf Process* 2018; 17: 137.

62. Chang W-L, Huang S-C and Lin KW. Fast parallel DNA-based algorithms for molecular computation: discrete logarithm. *J Supercomput* 2011; 56: 129–163.

63. Chang W-L, Guo M and Ho M-H. Fast parallel molecular algorithms for DNA-based computation: factoring integers. *IEEE Trans Nanobioscience* 2005; 4: 149–163.

64. Ning K. A pseudo DNA cryptography method. *arXiv preprint arXiv:09032693*. 2009.

65. Wang S, Wang C and Xu C. An image encryption algorithm based on a hidden attractor chaos system and the Knuth–Durstenfeld algorithm. *Opt Lasers Eng* 2020; 128: 105995.

66. Zhan K, Wei D, Shi J, et al. Cross-utilizing hyperchaotic and DNA sequences for image encryption. *J Electron Imaging* 2017; 26: 013021.

67. Zhen P, Zhao G, Min L, et al. Chaos-based image encryption scheme combining DNA coding and entropy. *Multimed Tools Appl* 2016; 75: 6303–6319.

68. Girdhar A and Kumar V. A RGB image encryption technique using Lorenz and Rossler chaotic system on DNA sequences. *Multimed Tools Appl* 2018; 77: 27017–27039.

69. Fan H, Li M, Liu D, et al. Cryptanalysis of a plaintext-related chaotic RGB image encryption scheme using total plain image characteristics. *Multimed Tools Appl* 2018; 77: 20103–20127.

70. Liu L, Zhang Q and Wei X. A RGB image encryption algorithm based on DNA encoding and chaos map. *Comput Electr Eng* 2012; 38: 1240–1248.

71. Wiggins S. *Introduction to applied nonlinear dynamical systems and chaos*. Springer-Verlag New York: Springer Science & Business Media, 2003.

72. Wolf A, Swift JB, Swinney HL, et al. Determining Lyapunov exponents from a time series. *Physica D* 1985; 16: 285–317.

73. Li C, Gong Z, Qian D, et al. On the bound of the Lyapunov exponents for the fractional differential systems. *Chaos* 2010; 20: 013127.

74. Frederickson P, Kaplan JL, Yorke ED, et al. The Liapunov dimension of strange attractors. *J Differ Equations* 1983; 49: 185–207.

75. Qi G, van Wyk MA, van Wyk BJ, et al. On a new hyperchaotic system. *Phys Lett A* 2008; 372: 124–136.

76. Dalkiran FY and Sprott JC. Simple chaotic hyperjerk system. *Int J Bifurcation Chaos* 2016; 26: 1650189.

77. Li C, Sprott JC, Thio W, et al. A new piecewise linear hyperchaotic circuit. *IEEE Trans Circuits Syst II Express Briefs* 2014; 61: 977–981.

78. Leutcho G, Kengne J and Kengne LK. Dynamical analysis of a novel autonomous 4-D hyperjerk circuit with hyperbolic sine nonlinearity: chaos, antimonotonicity and a plethora of coexisting attractors. *Chaos, Solitons Fractals* 2018; 107: 67–87.

79. Vaidyanathan S. Analysis, adaptive control and synchronization of a novel 4-D hyperchaotic hyperjerk system via backstepping control method. *Arch Control Sci* 2016; 26: 311–338.

80. Daltzis P, Vaidyanathan S, Pham VT, et al. Hyperchaotic attractor in a novel hyperjerk system with two nonlinearities. *Circuits Syst Signal Process* 2018; 37: 613–635.

81. Zhang S, Zeng YC and Jun Li Z. A novel four-dimensional no-equilibrium hyper-chaotic system with grid multiwing hyper-chaotic hidden attractors. *J Comput Nonlinear Dyn* 2018; 13(9): 090908.
82. Lin H, Wang C and Tan Y. Hidden extreme multistability with hyperchaos and transient chaos in a Hopfield neural network affected by electromagnetic radiation. *Nonlinear Dyn* 2020; 99: 2369–2386.

83. Mahmoud EE. Generation and suppression of a new hyperchaotic nonlinear model with complex variables. *Appl Math Modell* 2014; 38: 4445–4459.

84. Mahmoud EE. Dynamics and synchronization of new hyperchaotic complex Lorenz system. *Math Comput Modell* 2012; 55: 1951–1962.

85. Yang X and Cao J. Finite-time stochastic synchronization of complex networks. *Appl Math Modell* 2010; 34: 3631–3641.

86. Abdurahman A, Jiang H and Teng Z. Finite-time synchronization for memristor-based neural networks with time-varying delays. *Neural Netw* 2015; 69: 20–28.

87. Bao H and Cao J. Finite-time generalized synchronization of nonidentical delayed chaotic systems. *Nonlinear Anal Model Control* 2016; 21: 306–324.

88. Moulay E and Perruquetti W. Finite time stability and stabilization of a class of continuous systems. *J Math Anal Appl* 2006; 323: 1430–1443.

89. Goumidi DE and Hachouf F. Modified confusion-diffusion based satellite image cipher using chaotic standard, logistic and sine maps. In: 2010 2nd European Workshop on Visual Information Processing (EUVIP), Paris, France, 5–6 July 2010, pp.204–209. New York, NY: IEEE.

90. Tian Y and Lu Z. Novel permutation-diffusion image encryption algorithm with chaotic dynamic S-box and DNA sequence operation. *AIP Adv* 2017; 7: 085008.

91. Elamrawy F, Sharkas M and Nasser AM. An image encryption based on DNA coding and 2D Logistic chaotic map. *Int J Signal Process* 2018; 3: 27–32.

92. Sun S. Chaotic image encryption scheme using two-by-two deoxyribonucleic acid complementary rules. *Opt Eng* 2017; 56: 116117.

93. Stalin S, Maheshwary P, Shukla PK, et al. Fast and secure medical image encryption based on non linear 4D logistic map and DNA sequences (NL4DLM_DNA). *J Med Syst* 2019; 43: 267.

94. Shannon CE. Communication theory of secrecy systems. *Bell Syst Tech J* 1949; 28: 656–715.

95. Wu Y, Noonan JP and Agaian S. NPCR and UACI randomness tests for image encryption. *Cyber J* 2011; 1: 31–38.

96. Hashemi S, Pourmina MA, Mobayen S, et al. Design of a secure communication system between base transmitter station and mobile equipment based on finite-time chaos synchronisation. *Int J Syst Sci* 2020; 51: 1969–1986.

97. Vaseghi B, Pourmina MA and Mobayen S. Finite-time chaos synchronization and its application in wireless sensor networks. *Trans Inst Meas Control* 2018; 40: 3788–3799.

**Author biographies**

**Javad Mostafaee** was born in Abyek, Iran, in December 1982. Javad received the B.Sc. and M.Sc. degree in control engineering from Islamic Azad University (IAU), Qazvin Branch, Qazvin, Iran, in 2011 and 2015, respectively. He is currently working toward the Ph.D. degree in Control Engineering at Islamic Azad University (IAU), Saveh Branch. He is focusing on development and implementation of model robust control techniques on hyper-chaotic systems. His research interests include model robust control, Image encryption, chaotic, and hyper-chaotic systems and nonlinear analysis.
Saleh Mobayen received the B.Sc. and M.Sc. degrees in Control Engineering from the University of Tabriz, Tabriz, Iran, in 2007 and 2009, respectively, and received his Ph.D. in Control Engineering from Tarbiat Modares University, Tehran, Iran, in January 2013. From February 2013 to December 2018, he was as an Assistant Professor and faculty member with the Department of Electrical Engineering of University of Zanjan, Zanjan, Iran. Since December 2018, He is Associate Professor of Control Engineering at the Department of Electrical Engineering of University of Zanjan. Currently, he collaborates with National Yunlin University of Science and Technology as Associate Professor of Future Technology Research Center. He has published several papers in the national and international journals. He is a member of the Institute of Electrical and Electronics Engineers (IEEE), a member of the IEEE control systems society and serves as a member of program committee of several international conferences. Dr. Mobayen is the Associate Editor of Artificial Intelligence Review, Associate Editor of International Journal of Control, Automation and Systems, Associate Editor of Circuits, Systems, and Signal Processing, Associate Editor of Simulation, Associate Editor of Measurement and Control, Academic Editor of Complexity, Associate Editor of International Journal of Dynamics and Control, Academic Editor of Mathematical Problems in Engineering, Associate Editor of SN Applied Sciences, and other international journals. His research interests include control theory, sliding mode control, robust tracking, non-holonomic robots and chaotic systems.

Behrouz Vaseghi was born in Esfahan, Iran, in 1981. Behrouz received the B.Sc. and M.Sc. degree in electrical engineering from Islamic Azad University (IAU), Najafabad Branch, Esfahan, Iran, in 2004 and 2008, respectively. He received the Ph.D. degree in communication engineering from IAU, Science and Research Branch, Tehran, Iran, in 2017. Since 2009, he has been an academic member of the Department of Electrical Engineering, IAU, Abhar Branch. Since 2017, he has been an Assistant Professor with the Department of Electrical Engineering, IAU, Abhar Branch. His research interests include communication systems, audio and video processing, chaotic systems, chaotic cryptography and chaos synchronization.

Mohammad Vahedi is an Assistant Professor at Islamic Azad University of Saveh in Iran. He holds BS, MS, and PhD degrees in Mechanical Engineering from Amirkabir University of Technology, Shiraz University and Iran University of Science and Technology in Iran, respectively. He is now head of Department of Mechanical Engineering in Faculty of Engineering at Azad University of Saveh in Iran. His research interests are Vibration and Control, Robotic, Robust Control and Finite Element Method. He has published nearly 20 papers in the area of Vibration and Control, sliding mode control, Optimal control, Finite Element Method in various journals and conferences.

Afef Fekih (SM'07) received the BS, MS, and PhD degrees all in Electrical Engineering from the National Engineering School of Tunis, Tunisia in 1995, 1998, and 2002, respectively. Currently, she is a Full Professor in the Department of Electrical and Computer Engineering and the Chevron/BORSF Professor in Engineering at the University of Louisiana at Lafayette. Her research interests focus on control theory and applications, including nonlinear and robust control, optimal control, fault tolerant control with applications to power systems, wind turbines, unmanned vehicles, communication systems and automotive engines. Dr. Fekih is a senior member of the Institute of Electrical and Electronics Engineers (IEEE), a member of the IEEE control systems society, the IEEE women in control society and the IEEE Industrial electronics society.