IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received December 7, 2020, accepted January 21, 2021, date of publication January 29, 2021, date of current version February 8, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3055580

Finite Time Chaos Synchronization in Time-Delay Channel and Its Application to Satellite Image Encryption in OFDM Communication Systems

BEHROUZ VASEGHI[1], SEYEDEH SOMAYEH HASHEMI[1], SALEH MOBAYEN[2,3], (Member, IEEE), AND AFEF FEKIH[4], (Senior Member, IEEE)

[1]Department of Electrical and Computer Engineering, Abhar Branch, Islamic Azad University, Abhar 4561934367, Iran
[2]Department of Electrical Engineering, Faculty of Engineering, University of Zanjan, Zanjan 45371-38791, Iran
[3]Future Technology Research Center, National Yunlin University of Science and Technology, Yunlin 64002, Taiwan
[4]Department of Electrical and Computer Engineering, University of Louisiana at Lafayette, Lafayette, LA 70504-3890, USA

Corresponding author: Saleh Mobayen (mobayen@znu.ac.ir; mobayens@yuntech.edu.tw)

ABSTRACT This paper proposes a finite time chaos synchronization approach for the secure communication of satellite imaging. To this end, chaotic oscillators are considered in both the transmitter and receiver ends to generate the chaotic encryption/decryption keys. To mitigate the non-negligible channel time-delay between the receiver and transmitter, we propose a robust controller design. The proposed approach is designed based on the Lyapunov stability theory and the finite-time synchronization concept to attain finite time synchronization in a time-delayed channel. By using synchronized chaotic keys, a physical-layer chaotic encryption scheme for transmitting the satellite images is designed in orthogonal frequency-division multiplexing wireless network. The proposed chaotic-based satellite image encryption/decryption system is validated using a numerical simulation study. Additionally, to analyse the robustness and demonstrate the efficiency of the proposed chaotic encryption structure, a set of security analysis tools such as histogram analysis, key space analysis, correlation test, information entropy and other statistical analysis were performed.

INDEX TERMS Secure communication, chaos synchronization, finite-time stability, orthogonal frequency-division multiplexing.

I. INTRODUCTION

Over the past few decades we have witnessed a wide growth in information communication technology and its application in space sciences. Additionally, the internet has revolutionized communication and enabled information access with unprecedented ease. In this context, satellite image transmission and processing have widely been considered in remote sensing and earth observation [1]. For instance, satellite images are widely used in oceanography, meteorology, regional planning, biodiversity conservation, agriculture, cartography, forestry, geology and warfare. Satellite images have also been used to enable countries to monitor each other's actions in the field of nuclear activities, weapon deployment, and unauthorized activities. The security of satellite images, however, is of utmost importance. Satellite image encryption and privacy protection systems have been extensively applied in both commercial and military sectors. The history of modern data encryption goes back to 1945 when Claude Shannon of Bell Labs published an article entitled "A mathematical theory of cryptography" [2]. From the presentation of the first data encryption methods to nowadays, there has been huge developments in encryption techniques [3], [4]. Digital technology has replaced analogue encryption techniques and sophisticated algorithms have increased the efficiency of data encryption. Though conventional encryption schemes can actually satisfy the security constraints of multimedia information during transmission, there are still some limitations when it comes to protecting all multimedia content and preventing illegal access. For instance, several researchers have shown that these methods have some defects against brute-force attacks due to lower key space [5]. Also, in most cases, the traditional encryption methods require high computational power and long processing times [6]. In real-time usage

The associate editor coordinating the review of this manuscript and approving it for publication was Eyuphan Bulut.

and implementation such as wireless communication, due to the low speed of encryption and decryption, these drawbacks may result in considerable latency [7]. In this regard, cryptography using chaotic signals is a promising techniques which offers a good combination of security, speed and capability [8]. The above attributes along with the fast expansion in the application and theory of chaos [9], many researchers have recently focused on chaotic cryptography techniques. One of the most significant characteristics of chaotic signals is the fact that their behaviour closely mimics that of noise. Hence, this feature can be used to implement a data encryption system [10]–[12]. The implementation of encryption methods using chaotic systems is an expanding encryption technology which uses chaotic signals generated by chaotic systems to create keys in encryption systems [13], [14]. These chaotic keys have good features such as large key space and are extremely sensitive to the system parameters and initial states as a password [15], [16].

It is worth noting that chaotic signals exhibit interesting properties that have led to their deployment in various circuits [17]–[19]. In the communication domain, chaotic signals were introduced as broadband signals, sensitive to initial conditions, similar to noise, impulsive correlation, and low cross correlation between signals produced with different initial conditions [20]–[22]. Chaos is precisely employed in various communication applications such as radar [23], spread-spectrum systems [24], secure communication [25], ultra-wide-band communication [26] and video, image, and speech encryption [27]. Specially, in the field of multimedia encryption, because of the randomness and rich dynamics of chaotic systems, many encryption methods using chaos theory have been introduced [27]–[29]. These applications have been stimulated based on the chaotic system behaviours such as excessive dependence on system parameters and initial conditions, in addition to deterministic behaviours and complex dynamics [30]. Due to the little cost and great security attributes of the chaotic signals, implementation of cryptosystems for satellite image encryption using chaotic systems is an effective solution and they can perfectly resolve the security problems in this regard [31].

In order to ensure the secure, private and reliable transfer of satellite images, these latter must be encrypted in the downlink. To implement a secure chaotic communication system and generate the same keys in the encryptor and decryptor, the transmitter and receiver chaotic oscillators should be synchronized. The design of a controller and synchronizer for chaotic systems is key in the use of chaos as a mean of security in information transport. Carroll and Pecora have demonstrated experimentally and theoretically that if the chaotic system is modeled in a master-slave form, the two chaotic signals can be synchronized [32]. This finding has led to widening the potential applications of synchronized chaotic systems in communication and closing the gap between practical implementation of chaotic communication and chaos theory. In the aspect of chaos synchronization techniques, various approaches such as sliding mode control [33] digital redesign control [34], optimal control [35], backstepping method [28], impulsive control [36], intermittent scheme [37], switching process [38], composite nonlinear feedback [39] and neural-based control [40] can be considered. On the other hand, in realistic processes of chaotic communication systems, transmission delays ubiquitous. Additionally, their range is unknown in most systems. Strictly speaking, in the satellite communication application such as satellite imaging with consideration of the time delay propagation of communication channel, it is not necessary that the slave system is exactly synchronized with the master system. For instance, in telephone communication systems, the voice is created in the transmitter side at the moment t, whereas the receiver hears it at time $t - \tau$. Though the theoretical results of the chaos synchronization in secure communication in different senses without time-delay have been fruitfully established, the corresponding theoretical results of chaotic secure communication with time delay in channels is limited.

Based on the above discussion, we propose in this paper a chaos synchronization approach for the secure and reliable communication of satellite imaging. Its main contributions are as follows:

- It proposes an appropriate master-slave chaotic system for the encryption and transmitting the satellite images.
- It designs a robust controller to enable the synchronization of the state trajectories of the receiver chaotic oscillator at time t with the transmitter chaotic oscillator at time $t - \tau$ in the finite time.
- It suggests the combination of chaotic encryption method as multi-shift cipher encryption and chaotic masking for scrambling and shifting of Quadratic Amplitude Modulation (QAM) constellation to enhance the physical-layer security during Orthogonal Frequency Division Multiplexing (OFDM) data transmission.
- It successfully implements the proposed approach for the secure encryption/decryption of satellite images.

The remainder of the paper is organized as follows. The primary definition and mathematical model are presented in section II. The proposed control laws for the finite time synchronization in time-delayed channels are provided in Section III. The application to satellite image cryptosystem containing encryption and decryption is detailed in section IV. The performance of the proposed cryptosystem is illustrated in section V using both numerical simulations and security analysis tools. Finally, some concluding remarks are outlined in section VI.

II. PRIMARY DEFINITION AND MATHEMATICAL MODEL

Using the improved Chua oscillator [41], the resultant transmitter chaotic system as the master system can be described as

$$\begin{aligned} \dot{x}_1(t) &= \alpha(x_2(t) - f(x_1(t))) \\ \dot{x}_2(t) &= x_1(t) - x_2(t) + x_3(t) \\ \dot{x}_3(t) &= -\eta x_2(t) \end{aligned} \tag{1}$$

with nonlinear bounded function $f(x_1(t)) = -sin(x_1(t))$ $exp(-0.1\,|x_1(t)|)$, where $x_1(t)$, $x_2(t)$ and $x_3(t)$ denote the states of the slave system. The suitable non negative unvarying parameters α and η confirm that the chaotic behavior occurs in the modified Chua system.

Moreover, the receiver chaotic oscillator as the slave system with parametric uncertainties is considered as

$$\begin{aligned}\dot{y}_1(t) &= \lambda sgn(x_1(t) - y_1(t))\\ \dot{y}_2(t) &= y_1(t) - y_2(t) + y_3(t) + u_1(t)\\ \dot{y}_3(t) &= -(\eta - \Delta\eta(t))y_2(t) + u_2(t)\end{aligned}\tag{2}$$

where $y_1(t)$, $y_2(t)$ and $y_3(t)$ are the slave system states; η is a constant parameter; λ is the design parameter; $u_1(t)$ and $u_2(t)$ are two control input signals, and $\Delta\eta(t)$ is the time varying parametric uncertainty.

Assumption 1: The time varying parametric uncertainty $\Delta\eta(t)$ is supposed bounded as follow:

$$|\Delta\eta(t)| \leq \delta \tag{3}$$

where δ is a positive constant.

As can be seen from Eq. (2), the first term of this equation contains $x_1(t)$ as the first output of master oscillator. In fact, the slave system becomes chaotic when it receives this signal. Now, considering the time delay propagation τ in communication channel and replacing $x_1(t)$ by $x_1(t-\tau)$, the dynamics of the slave system is given by

$$\begin{aligned}\dot{y}_1(t) &= \lambda sgn(x_1(t-\tau) - y_1(t))\\ \dot{y}_2(t) &= y_1(t) - y_2(t) + y_3(t) + u_1(t)\\ \dot{y}_3(t) &= -(\eta - \Delta\eta(t))y_2(t) + u_2(t)\end{aligned}\tag{4}$$

That is, if we consider t as the base of time in the receiver slave system, therefore the received dynamics from the transmitter master system can be considered as

$$\begin{aligned}\dot{x}_1(t-\tau) &= \alpha(x_2(t-\tau) - f(x_1(t-\tau)))\\ \dot{x}_2(t-\tau) &= x_1(t-\tau) - x_2(t-\tau) + x_3(t-\tau)\\ \dot{x}_3(t-\tau) &= -\eta x_2(t-\tau)\end{aligned}\tag{5}$$

The synchronization errors between the slave chaotic system (4) and master chaotic system (5) at the receiver side are defined as

$$\begin{aligned}e_1(t) &= y_1(t) - x_1(t-\tau)\\ e_2(t) &= y_2(t) - x_2(t-\tau)\\ e_3(t) &= y_3(t) - x_3(t-\tau)\end{aligned}\tag{6}$$

Definition 1: Consider the slave and master systems (4) and (5), respectively. If there exists a time $T_1 > 0$ so that the following condition is met:

$$\lim_{t\to T_1} \|E(t)\| = \lim_{t\to T_1} \|Y(t) - X(t-\tau)\| = 0 \tag{7}$$

where $X(t-\tau) = [x_1(t-\tau), x_2(t-\tau), x_3(t-\tau)]^T$, $Y(t) = [y_1(t), y_2(t), y_3(t)]^T$ and $E(t) = [e_1(t), e_2(t), e_3(t)]^T$ then, the finite-time synchronization of the states of systems (4) and (5) is achieved. Strictly speaking, the controller inputs $u_1(t)$ and $u_2(t)$ use the output error signal between the slave oscillator at time t and master oscillator at time $t-\tau$, i.e., $Y(t) - X(t-\tau)$, which is physically implementable.

Lemma 1 [42]: For the positive real numbers ε_1, ε_2 and k with $0 \leq k \leq 1$, the subsequent inequality is acquired:

$$(|\varepsilon_1| + |\varepsilon_2|)^k \leq |\varepsilon_1|^k + |\varepsilon_2|^k \tag{8}$$

Lemma 2 [43]: Assume that A and B are n-dimensional vectors and ϖ is a positive constant. Then, the subsequent result is obtained

$$2A^TB \leq \varpi A^TA + \varpi^{-1}B^TB \tag{9}$$

Lemma 3 [44]: Consider $V(t)$ as a positive-definite continuous function and real numbers $0 < \xi < 1$ and $\kappa > 0$ where

$$\dot{V}(t) \leq -\kappa V(t)^{\xi}, \quad \forall t \geq t_0,\ V(t_0) \geq 0 \tag{10}$$

then, the next results are obtained:

$$V(t)^{1-\xi} \leq V(t_0)^{1-\xi} - \kappa(1-\xi)(t-t_0), \quad t_0 \leq t \leq T_1 \tag{11}$$

and

$$V\,(t) \equiv 0 \quad \forall t \geq T_1 \tag{12}$$

where the settling time T_1 is given by

$$T_1 = t_0 + \frac{V(t_0)^{1-\xi}}{\kappa(1-\xi)}. \tag{13}$$

III. FINITE TIME CHAOS SYNCHRONIZATION

The dynamics of synchronization errors between the receiver chaotic oscillator and the transmitter chaotic oscillator is achieved by differentiating (6) and subtracting (5) from (4) as follows:

$$\begin{aligned}\dot{e}_1(t) &= \lambda sgn(-e_1(t)) - \alpha(x_2(t-\tau) - f(x_1(t-\tau)))\\ \dot{e}_2(t) &= e_1(t) - e_2(t) + e_3(t) + u_1(t)\\ \dot{e}_3(t) &= -\eta e_2(t) + \Delta\eta y_2(t) + u_2(t)\end{aligned}\tag{14}$$

To solve the synchronization problem, our purpose is to obtain the controller signals $u_1(t)$ and $u_2(t)$ so that the variable states of receiver oscillator are synchronized with the variable states of transmitter oscillator in finite time. This control objective is equivalent to obtaining controller signals $u_1(t)$ and $u_2(t)$ so as to attain the stability of the error dynamics (14) in finite time. For this purpose, we propose the cascade synchronization procedure, where the error dynamic system (14) is converted to two subsystems as follow:

$$\dot{e}_1(t) = \lambda sgn(-e_1(t)) - \alpha(x_2(t-\tau) - f(x_1(t-\tau))) \tag{15}$$

and

$$\begin{aligned}\dot{e}_2(t) &= e_1(t) - e_2(t) + e_3(t) + u_1(t)\\ \dot{e}_3(t) &= -\eta e_2(t) + \Delta\eta y_2(t) + u_2(t)\end{aligned}\tag{16}$$

In actuality, the error signal $e_1(t)$ is used as an "external" input to the synchronization error dynamics $\dot{e}_2(t)$ and $\dot{e}_3(t)$.

Theorem 1: Consider the error dynamic subsystem expressed by (15). This subsystem is finite-time stable and there is a constant finite time T_1 such that $e_1(t) \equiv 0$ is obtained for $t \geq T_1$ given by

$$T_1 \leq \frac{\left(\frac{1}{2}e_1^2(0)\right)^{1-\xi_1}}{\kappa_1(1-\xi_1)}. \tag{17}$$

Proof: The candidate Lyapunov function $V_1(e_1(t))$ is considered as

$$V_1(e_1(t)) = \frac{1}{2}e_1^2(t). \tag{18}$$

By computing the time-derivative of $V_1(e_1(t))$, one has

$$\begin{aligned}\dot{V}_1(e_1(t)) &= e_1(t)\,\dot{e}_1(t)\\ &= \lambda sgn(-e_1(t))e_1(t) - \alpha x_2(t-\tau)e_1(t)\\ &\quad + \alpha f(x_1(t-\tau))e_1(t)\\ &= -\lambda\,|e_1(t)| - \alpha x_2(t-\tau)\,e_1(t)\\ &\quad + \alpha f(x_1(t-\tau))e_1(t).\end{aligned} \tag{19}$$

According to the condition $|f(x_1(t-\tau))| \leq 1, \forall t \geq 0$ and $|x_2(t-\tau)| \leq \theta, \forall t \geq 0$, one obtains

$$\begin{aligned}\dot{V}_1(e_1(t)) &\leq -\lambda\,|e_1(t)| - \alpha\theta e_1(t) + |\alpha|\cdot 1\cdot |e_1(t)|\\ &\leq -\lambda\,|e_1(t)| - \alpha\theta e_1(t) + \alpha\,|e_1(t)|\\ &\leq -|e_1(t)|\,(\lambda - \alpha(1-\theta)).\end{aligned} \tag{20}$$

Now, if and only if $\lambda > \alpha(1-\theta)$, by choosing $\kappa_1 = \sqrt{2}$ and $\xi_1 = 0.5$, one can find:

$$\dot{V}_1(e_1(t)) \leq -|e_1(t)| = -\kappa_1 V_1(e_1(t))^{\xi_1}. \tag{21}$$

Thus, by applying Lemma 2, the error dynamic subsystem (15) is finite-time stable. Thus, the proof is completed. □

When $t > T_1$, we have $e_1(t) \equiv 0$ and Eq. (16) converts to

$$\begin{aligned}\dot{e}_2(t) &= -e_2(t) + e_3(t) + u_1(t)\\ \dot{e}_3(t) &= -\eta e_2(t) + \Delta\eta y_2(t) + u_2(t)\end{aligned} \tag{22}$$

Theorem 2: The error subsystem (22) is considered.Using the control laws $u_1(t)$ and $u_2(t)$ as

$$u_1(t) = -r_1 e_2(t) - e_2^{\gamma}(t) \tag{23}$$

$$u_2(t) = -r_2 e_3(t) - e_3^{\gamma}(t) - \mu\,|y_2(y)|\,sgn(e_3(t)) \tag{24}$$

where $\mu \geq \delta$, $\gamma = q/p$, $p > q$, p and q are two positive odd numbers, and r_1, r_2 denote the control gains which will be specified later, then the error dynamical subsystem (22) is finite-time stable and there is a constant finite time T_2 so that $e_2(t) \equiv e_3(t) \equiv 0$ is obtained for $t \geq T_2$ given by

$$T_2 \leq \frac{\left[\frac{1}{2}\sum_{j=2}^{3} e_j^2(0)\right]^{1-\xi_2}}{\kappa_2(1-\xi_2)}. \tag{25}$$

Proof: Choose the Lyapunov candidate function $V_2(e(t))$ as

$$V_2(e(t)) = \frac{1}{2}\sum_{j=2}^{3} e_j^2(t) \tag{26}$$

where differentiating $V_2(e(t))$ yields

$$\dot{V}_2(e(t)) = \sum_{j=2}^{3} e_j(t)\dot{e}_j(t). \tag{27}$$

By replacing $\dot{e}_j(t)$ from (22) into (27), one has:

$$\begin{aligned}\dot{V}_2(e(t)) = &\left(e_3(t)e_2(t) + u_1(t)e_2(t) - e_2^2(t)\right)\\ &+ \left(\Delta\eta(t)y_2(t)e_3(t) + u_2(t)e_3(t) - \eta e_2(t)e_3(t)\right).\end{aligned} \tag{28}$$

Now, by using the control lows $u_1(t)$ and $u_2(t)$, we have

$$\begin{aligned}\dot{V}_2(e(t)) &= e_2(t)e_3(t) - e_2^2(t) - r_1 e_2^2(t) - e_2^{\gamma+1}(t)\\ &\quad - \eta e_2(t)e_3(t) + \Delta\eta(t)y_2(t)e_3(t) - r_2 e_3^2(t)\\ &\quad - e_3^{\gamma+1}(t) - \mu\,|y_2(t)|\,sgn(e_3(t))e_3(t)\\ &\leq e_2(t)e_3(t) - (1+r_1)e_2^2(t) - e_2^{\gamma+1}(t)\\ &\quad - \eta e_2(t)e_3(t) - r_2 e_3^2(t) - e_3^{\gamma+1}(t)\\ &\quad - (\mu - \Delta\eta(t)sgn(y_2(t)e_3(t)))\,|y_2(t)e_3(t)|\\ &\leq e_2(t)e_3(t)(1-\eta) - (1+r_1)e_2^2(t)\\ &\quad - e_2^{\gamma+1}(t) - e_3^{\gamma+1}(t) - r_2 e_3^2(t)\end{aligned} \tag{29}$$

where based on Eq. (9) in Lemma 2, Eq. (29) is simplified as

$$\begin{aligned}\dot{V}_2(e(t)) &\leq -e_2^2(t)(1+r_1) + \left(\frac{|1-\eta|}{2}\varpi e_2^2(t) + \frac{|1-\eta|}{2\varpi}e_3^2(t)\right)\\ &\quad - r_2 e_3^2(t) - e_2^{\gamma+1}(t) - e_3^{\gamma+1}(t)\\ &\leq -e_2^2(t)\left(1 + r_1 + \frac{|1-\eta|}{2}\varpi\right) - e_3^2(t)\left(r_2 - \frac{|1-\eta|}{2\varpi}\right)\\ &\quad - e_2^{\gamma+1}(t) - e_3^{\gamma+1}(t)\end{aligned} \tag{30}$$

If the gains r_1 and r_2 are determined as

$$r_1 \geq \frac{|1-\eta|}{2}\varpi - 1 \ and\ r_2 \geq \frac{|1-\eta|}{2\varpi} \tag{31}$$

Then, using Lemma 1, Eq. (30) is converted to

$$\begin{aligned}\dot{V}_2(e(t)) &\leq -e_2^{\gamma+1}(t) - e_3^{\gamma+1}(t)\\ &= -2^{\frac{\gamma+1}{2}}\left(\frac{1}{2}e_2^2(t)\right)^{\frac{\gamma+1}{2}} - 2^{\frac{\gamma+1}{2}}\left(\frac{1}{2}e_3^2(t)\right)^{\frac{\gamma+1}{2}}\\ &= -2^{\frac{\gamma+1}{2}}\left(\left(\frac{1}{2}e_2^2(t)\right)^{\frac{\gamma+1}{2}} + \left(\frac{1}{2}e_3^2(t)\right)^{\frac{\gamma+1}{2}}\right)\\ &\leq -2^{\frac{\gamma+1}{2}}\left(\frac{1}{2}e_2^2(t) + \frac{1}{2}e_3^2(t)\right)^{\frac{\gamma+1}{2}}\\ &= -\kappa_2 V_2(e(t))^{\xi_2}\end{aligned} \tag{32}$$

with $\kappa_2 = 2^{\frac{\gamma+1}{2}}$, $\xi_2 = \frac{\gamma+1}{2}$. Therefore, from Lemma 3, the error dynamics (22) is finite time stable. It means that the conditions $e_2(t) = 0$ and $e_3(t) = 0$ are obtained after a finite time T_2. This completes the proof. □

Consequently, when $t > T_2 > T_1$, one obtains

$$\begin{aligned}e_1(t) &= y_1(t) - x_1(t-\tau) = 0\\ e_2(t) &= y_2(t) - x_2(t-\tau) = 0\\ e_3(t) &= y_3(t) - x_3(t-\tau) = 0\end{aligned} \tag{33}$$

Therefore, it can be said that with the existence of the time delay propagation τ in communication channel, chaotic signals of slave oscillator (5) are synchronized with the chaotic signals of master oscillator (4) at the receiver side via the control inputs (23) and (24) in finite time.

IV. APPLICATION IN SATELLITE IMAGE ENCRYPTION

The block diagram of the proposed secure OFDM communication system for satellite image transmission is illustrated in Fig.1.

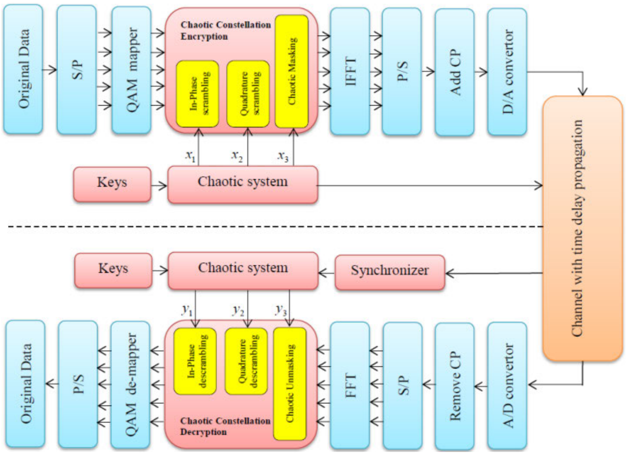


FIGURE 1. Block diagram of the proposed chaotic communication system using OFDM technique.

The system consists of a satellite downlink transmitter, 35600 Km standard downlink path in 4000 MHz frequency, free space path loss, and ground station downlink receiver. Note that comprehensiveconcepts of the OFDM technique for wireless multimedia communications can be found in [45]. In this section, our emphasis is on satellite image cryptosystem and the effect of the satellite channel.

A. SATELLITE IMAGE ENCRYPTION

The proposed encryption method is illustrated as follow:

Step 1: At first, the initial states and parameters of the modified Chua chaotic oscillator at the satellite downlink transmitter is defined. Then, the sampling interval of the system (Δh) is specified and the chaotic system is solved by using the fourth-order Range–Kutta (RK-4) integration algorithm and considering this sampling value. As a result of the system analysis, three chaotic signals as 15 digit float values $[x_1(i), x_2(i), x_3(i)]$ are obtained.

Step 2: By using the chaotic sequences $x_1(i)$, $x_2(i)$ and $x_3(i)$, the Chaotic keys $k_1(i)$, $k_2(i)$ and $k_3(i)$ are obtained as follows:

$$\begin{aligned} k_1\left(i\right) &= mod(x_1\left(i\right), floor(x_1(i-1))) \\ k_2(i) &= mod(x_2(i), floor(x_2(i-1))) \\ k_3(i) &= mod(x_3(i), floor(x_3(i-1))) \end{aligned} \tag{34}$$

where the function $mod(f, g)$ gives the residual of f divided by g, and $floor(\omega)$ produces the round of ω to the nearest integers.

Step 3: In the satellite downlink transmitter, the satellite image as the original data stream is transformed to a Serial-to-Parallel (S/P) data. After serial to parallel conversion, the data is sent to the QAM mapper who maps the data to the constellation points and the QAM symbols are achieved. The In-phase (I) component and the Quadrature (Q) component of QAM symbols can be separated and sent for chaotic constellation encryption.

Step 4: In the chaotic constellation encryption block, at first, by using the chaotic keys k_1 and k_2, the original constellation points I and Q are scrambled and shifted to a new constellation point I' and Q' by applying multi-shift cipher algorithm as [46]:

$$C(I(i)) = \underbrace{h(\ldots h(}_{n}h(I(i), k_1(i)), \underbrace{k_1(i)), \ldots, k_1(i))}_{n} = I'(i) \tag{35}$$

$$C(Q(i)) = \underbrace{h(\ldots h(}_{n}h(Q(i), k_2(i)), \underbrace{k_2(i)), \ldots, k_2(i))}_{n} = Q'(i) \tag{36}$$

where $h(.)$ is a piecewise function defined by

$$\begin{aligned} &h(J(i), K(i)) \\ &\quad = \begin{cases} (J\ (i) + K\ (i)) + 2l & -2l \leq (J(i) + K(i)) \leq -l \\ (J\ (i) + K\ (i)) & -l \leq (J(i) + K(i)) \leq l \\ (J\ (i) + K\ (i)) - 2l & l \leq (J(i) + K(i)) \leq 2l \end{cases} \end{aligned} \tag{37}$$

and l is chosen such that $J(i)$ and $K(i)$ are placed within the interval $[-l, l]$.

Lastly, the scrambled symbols I' and Q' are masked with the chaotic key k_3 and the final encrypted QAM symbols $I'' = I' + k_3$ and $Q'' = Q' + k_3$ are obtained. Then, the state signals $X(t)$ of the chaotic system at the satellite downlink transmitter and encrypted QAM symbols I'' and Q'' are sent to the ground satellite receiver via OFDM technique in a wireless channel with the time delay propagation. Fig.2 illustrates the concept of proposed chaotic constellation encryption using 16-QAM as an example.

The standard and encrypted 16-QAM constellations are plotted in Fig.2 (a) and (b), correspondingly. In the proposed encryption technique, the chaotic mapping causes a one-to-many function in comparison with the standard 16-QAM mapping. As Fig.2 (b), in the proposed method, any of the QAM symbol can be sited in the any location on the constellation that is predetermined by the chaotic keys k_1, k_2 and k_3. For the high number of data input, the range of constellation is filling out completely by the chaotic QAM symbol mapping. As a result, noise-like constellation extremely increases the security level owing to the random behavior, inherent scrambling and independent mapping of QAM symbols.

B. SATELLITE IMAGE DECRYPTION

For the image decryption at the ground satellite receiver, the chaotic keys $\tilde{k}_1(i)$, $\tilde{k}_2(i)$ and $\tilde{k}_3(i)$ should be corresponding

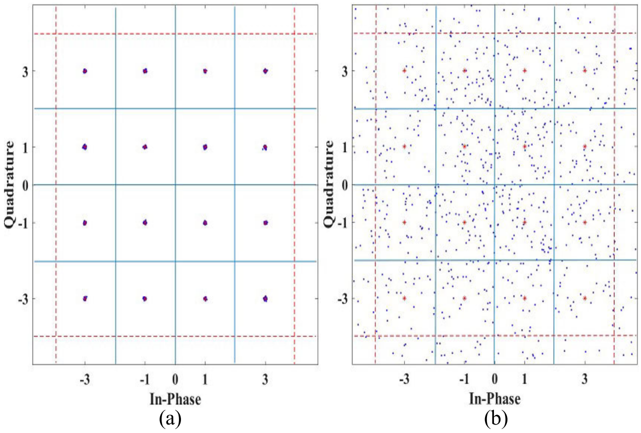


FIGURE 2. **Constellation mapping in 16-QAM, (a) Conventional mapping; (b) Chaotic mapping.**

to the encryption process at the satellite transmitter. When the synchronization purpose is achieved, the signals $y_1(t)$, $y_2(t)$ and $y_3(t)$ at the ground satellite receiver are synchronized with the received signals $x_1(t-\tau)$, $x_2(t-\tau)$ and $x_3(t-\tau)$, and the original satellite image can be recovered by applying a reverse operations in the encryption process, as follow:

Step 1: By using the chaotic sequences $y_1(i)$, $y_2(i)$ and $y_3(i)$, the keys $\tilde{k}_1(i)$, $\tilde{k}_2(i)$ and $\tilde{k}_3(i)$ are obtained as follows:

$$\begin{aligned}\tilde{k}_1(i) &= mod(y_1(i), floor(y_1(i-1)))\\ \tilde{k}_2(i) &= mod(y_2(i), floor(y_2(i-1)))\\ \tilde{k}_3(i) &= mod(y_3(i), floor(y_3(i-1)))\end{aligned} \tag{38}$$

Step 2: In the chaotic constellation decryption block, at first the chaotic key $\tilde{k}_3$ is subtracted from the encrypted symbols $I^{''}$ and $Q^{''}$ and unmasked symbols $I' = I^{''} - \tilde{k}_3$ and $Q' = Q^{''} - \tilde{k}_3$ are obtained. Now, by replacing I by I' and k_1 by $-\tilde{k}_1$ in (35) and also replacing Q by Q' and k_2 by $-\tilde{k}_2$ in (36), the decrypted QAM symbols are found as:

$$\begin{aligned}D(I'(i)) &= \underbrace{h(\ldots h(h}_{n}(I'(i), -\tilde{k}_1(i)), \underbrace{-\tilde{k}_1(i)), \ldots, -\tilde{k}_1(i))}_{n}\\ &= I(i)\end{aligned} \tag{39}$$

$$\begin{aligned}D(Q'(i)) &= \underbrace{h(\ldots h(h}_{n}(Q'(i), -\tilde{k}_2(i)), \underbrace{-\tilde{k}_2(i)), \ldots, -\tilde{k}_2(i))}_{n}\\ &= Q(i)\end{aligned} \tag{40}$$

Finally, the decrypted symbols are sent to the QAM de-mapper and after a P/S conversion, the correct satellite image is obtained from a scrambled and noisy-like constellation.

Remark 1: Although the slave and master chaotic oscillators are continuous and consequently the generated chaotic signals are continuous, however the MATLAB software is employed for implementation and as mentioned in step 1 of subsection *A*, the discrete chaotic sequences of cryptosystem are obtained directly from solver RK-4. Also, in real-world implementation context, we can use an Analog to Digital Convertor (ADC) to get the discrete chaotic sequences for cryptosystem.

Remark 2: In most of existing image encryption methods such as TD-ERCS based confusion and diffusion, dynamic S-Box; encryption process is applied on the image pixels (value or position, etc.). Although these methods are able to successfully hide the image information [28], [47], [48], for data communication networks, this process should be done at higher layers such as the media access control (MAC) layer. Data encryption at MAC layer encrypts the data but leaves the header untouched. In our proposed method, encryption is done on the QAM symbols at the physical layer. The physical layer encryption schemes are required to encrypt the entire data including the header for secure data transmission. Moreover, in the proposed scheme, the mapping for each QAM symbol is independent of other QAM symbols. Each QAM symbol can be located anywhere on the constellation. With the increase in the number of OFDM input signals, the final constellation range is filled entirely by the dynamic QAM symbol mapping. The resulting noise-like constellation strongly enhances the security level, due to the random, independent mapping and inherent scrambling of QAM symbols.

V. SIMULATION RESULTS

A. SIMULATION RESULTS OF CHAOS SYNCHRONIZATION

In this section, numerical simulation is presented to investigate the robustness, and precision of the proposed controllers for finite time chaos synchronization in time-delay channel. In this simulation, the satellite transmitter chaotic system(1) is considered with initial condition $(x_1(0), x_2(0), x_3(0)) = (15, 0, -15)$ and system parameters $\alpha = 9.35$ and $\eta = 14.65$. The satellite receiver chaotic system (2) is specified with initial condition $(y_1(0), y_2(0), y_3(0)) = (18, 2, -18)$ and system parameters $\lambda = 100$ and $\eta = 14.65$. Also, the channel time delay propagation is set to $\tau = 5s$ and the time-varying uncertainty parameter is assumed as

$$\Delta\eta(t) = 0.5\ sin(y_1 t) + 0.8\ cos(y_2 + y_3\sqrt{t}) \tag{41}$$

In Figs. 3-5, the states of the chaotic oscillators in the satellite receiver and transmitter are illustrated when the suggested controllers (23) and (24) are applied. It is seen that the chaotic signals $y_1(t)$ and $x_1(t)$ are synchronized in 0.001 second. Also, the states $y_2(t)$ and $y_3(t)$ are synchronized with $x_2(t)$ and $x_3(t)$ in 0.02 and 0.0004 seconds, respectively. Fig.6 indicates the error signals. It is shown from Fig.6 that the error signals approach zero in less than 0.01 second. So, it is concluded that the offered method is capable to dominate the parametric uncertainties effects which display the suitable synchronization performance of the suggested control approach. In Fig.7,time responses of the designed controller signals $u_1(t)$ and $u_2(t)$ are shown. From Fig.7, it is found that the amplitude of the proposed control signals is proper and no chattering problem has occurred in the control inputs.

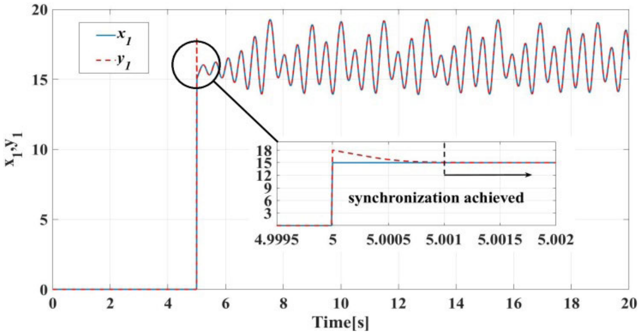


FIGURE 3. Time histories of x_1 and y_1 using the suggested controllers.

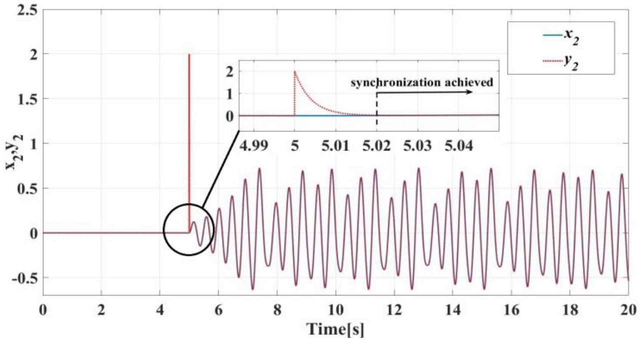


FIGURE 4. Time histories of x_2 and y_2 using the suggested controllers.

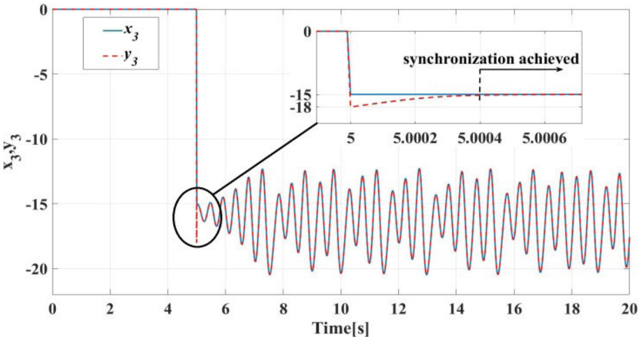


FIGURE 5. Time histories of x_3 and y_3 using the suggested controllers.

B. SIMULATION RESULTS OF SATEILLITE IMAGE ENCRYPTION

This section highlights the application of the proposed scheme to satellite image encryption for 35600 Km standard Downlink Path in 4000 MHz frequency and free space path loss. A Boston satellite image of size 1400 × 700 × 3 uint 8, in JPG format is used in this simulation as the original data which should be encrypted (see Fig.8 (a)). The encryption keys are generated by the transmitter chaotic oscillator. The original image is encrypted by applying these chaotic keys and the encryption method described in section IV-A. Fig.8 (b) shows the obtained encrypted Boston satellite image. At the receiver side, the chaotic oscillator is applied to produce the secret keys for decryption. After the synchronization procedure and above-mentioned

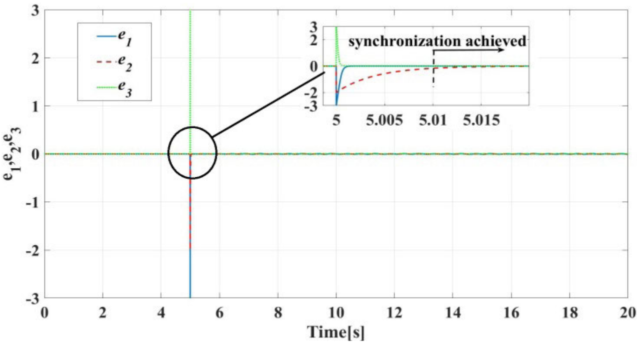


FIGURE 6. Time response of the error signals with the suggested controllers.

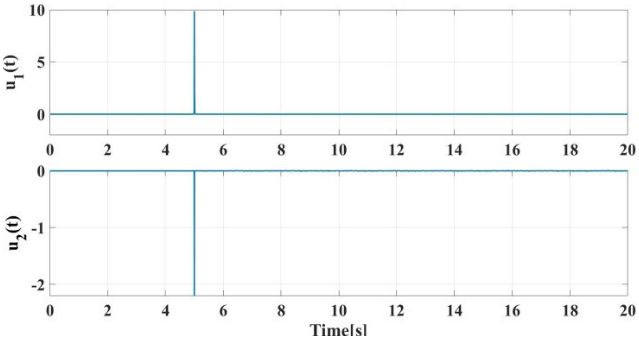
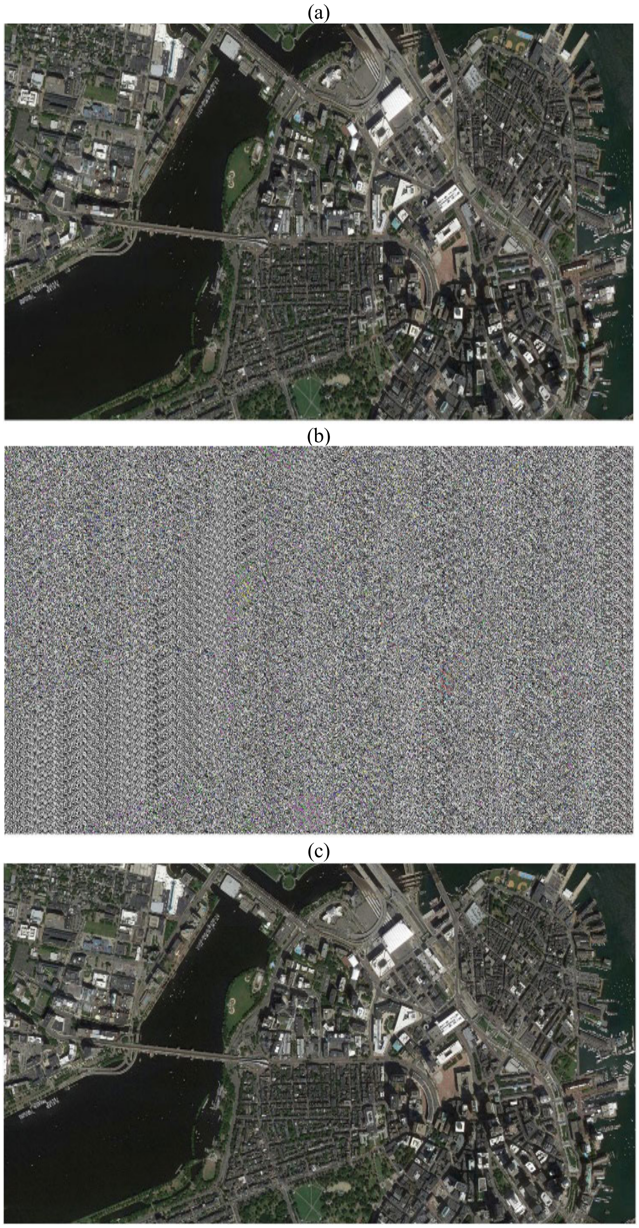


FIGURE 7. Time responses of control inputs, (a) $u_1(t)$, (b) $u_2(t)$.

decryption method, the decrypted Boston satellite image can be recovered (see Fig.8 (c)). It is evident from these figures, the encrypted satellite image has a uniform distribution, and the encrypted image is similar to the noise. This shows that from the viewpoint of visual impression, the suggested method has a well encryption performance.

To evaluate the effect of the satellite channel on the performance of the proposed system, the bit error ratio (BER) and the corresponding constellation diagrams is shown in Fig.9. From the BER curves it can be seen that, with correct security keys, the proposed chaotic OFDM schemes and original OFDM show nearly the same performance. The fact indicates that legitimate receiver can correctly recover the encrypted OFDM signal. The BER are about 0.3 for the entire signal to noise ratio when the signal is decrypted by illegal receivers.

On the other hand, High peak-to-average power ratio (PAPR) is a key drawback of the OFDM signal. Some encryption schemes can jointly reduce the PAPR in addition to the security enhancement [49]. The complementary commutative distribution function (CCDF) of PAPR curves measurements of 16-QAM OFDM transmission for the original and encrypted OFDM signals are shown in Fig.10. We can see from the figure that Compared to the original signal the encrypted signal has a lower PAPR. The fact indicates that in the proposed method no additional transmission performance degradation.


(a)

(b)

(c)

FIGURE 8. (a) Original image, (b) Encrypted image, (c) Decrypted image with exact keys.

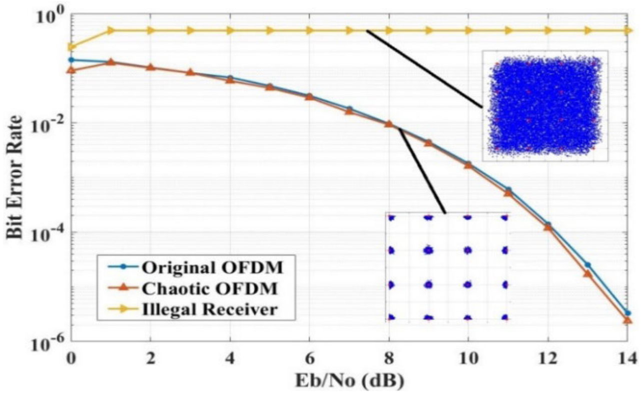


FIGURE 9. BER curves and the corresponding constellation diagrams for original OFDM, chaotic OFDM and illegal receiver.

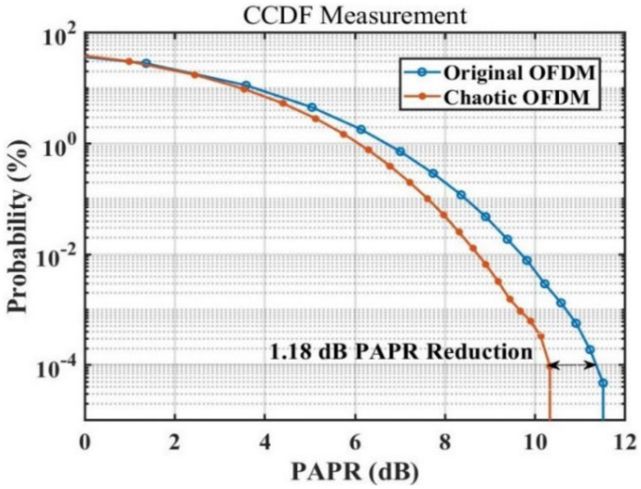


FIGURE 10. CCDF of PAPR for original and encrypted OFDM signals.

C. PERFORMANCE ANALYSIS OF THE DESIGNED CRYPTOSYSTEM

To illustrate the adequate security of the designed chaotic cryptosystem, we perform a set of security analysis tests. Key space analysis, histogram analysis, correlation test, Information Entropy (IE), the Number of Pixels Change Rate (NPCR) and Unified Average Changing Intensity (UACI) are carried out. Moreover, In order to show our innovations and efficiency for image encryption, the Irregular deviation, Maximum deviation, Energy analysis, Contrast test, Homogeneity test, Noise attack analysis, Cropping attack analysis, ciphertext only, known plaintext, chosen ciphertext, and chosen plaintexthave been done.

- *Analysis of key space*

The key space size for a cryptosystem is based on the total number of various keys that are utilized in encryption. A high-performance cryptosystem should possess a key space which is large enough to resist all types of brute-force attacks. These types of attacks are actually based on the exhaustive key search. In the proposed algorithm, if the eavesdropper wants to extract the original satellite image from the encrypted image, he/she will require the system parameters α and η, the initial states $x_1(0)$, $x_2(0)$, $x_3(0)$ of transmitter chaotic system (Eq.(1)) and the synchronization parameters r_1, r_2, γ, μ of Eqs. (23) and (24) 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 $(10^{14})^9 = 10^{126} \approx 2^{419}$. Thus, it is confirmed that the planned algorithm contains a large key-space which is capable sufficient to resist all possible types of statistical attacks.

- *Histograms Analysis*

To barricade the revelation of image information by an eavesdropper, it is as well as useful if the encrypted image has no or very few statistical similarities to the original image. The

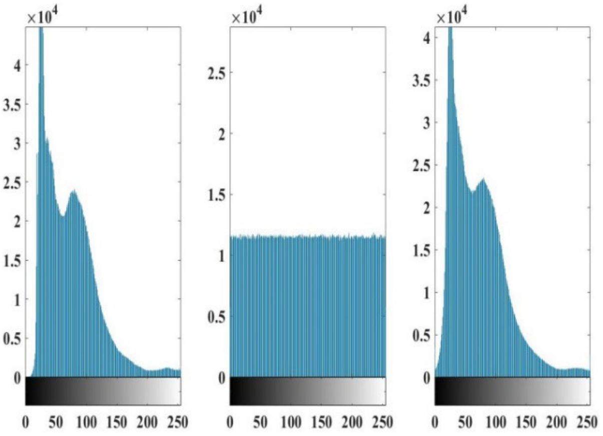


FIGURE 11. Histograms of (a) Original image, (b) Encrypted image, (c) Decrypted image.

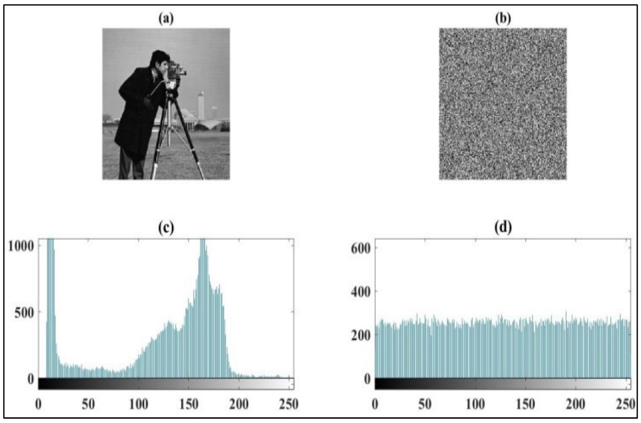


FIGURE 12. Encryption results for cameraman. (a) original image. (b) encrypted image. (c), (d) corresponding histograms.

histogram of image operates as a graphical display of tonal distribution in the digital image. The criterion of action is the level of brightness intensity in the pixels. Observing the histogram for a specific image, a viewer is capable to judge the whole tonal distribution at a glance.

The histograms of the original, encrypted and decrypted Boston satellite images are illustrated in Fig.11(a), Fig.11(b) and Fig.11(c), correspondingly. Additionally, to further compare our approach to other works, we consider a classical standard test image (cameraman) of size 256 × 256 uint 8. The result of the encryption process and its histograms for the cameraman are illustrated in Fig.12. The histograms of the encrypted images are more uniform, considerably different than the original images and have no statistical similarity to the original images. Therefore, it can be said that the proposed encryption method successfully hides the information of original images.

Moreover, the variance of a histogram can quantitatively describe the distribution of pixel values, which is calculated by [50]:

$$var(Z) = \frac{1}{n^2}\sum_{i=1}^{n-1}\sum_{j=1}^{n-1}\frac{1}{2}\left(z_i - z_j\right)^2 \qquad (42)$$

where Z is a vector and $Z = \{z_1, z_2, \ldots, z_{256}\}$, $\mathrm{z_i}$ and z_j are the numbers of pixels with gray values equal to i and j, respectively. The lower value of variance indicates the higher uniformity of ciphered images. In the experimental tests, the variances of the histograms of the Boston satellite image, cameraman image and their encrypted images are calculated by using Equation (42) and listed in TABLE 1. From TABLE 1, it can be discovered that the histogram variance values of the encrypted images are much smaller than those of the original images. Thus, our proposed algorithm has suitable performance in resisting statistical attacks.

TABLE 1. Variance of histogram.

Image	Original Image	Encrypted Image	Encrypted Image [50]
Boston	27281977.27	49826.68	-
Cameraman	111408.49	928.35	845.16

- *Correlation test*

A beneficial gauge to measure the encryption quality of an encryption system is the correlation coefficient between two adjacent sample values in the original message or the encrypted message. The correlation metric is calculated by

$$Corr(u, v) = \frac{cov(u, v)}{\sqrt{G(u)}\sqrt{G(v)}} \qquad (43)$$

$$Cov(u, v) = {}^1\!/_N \sum_{i=1}^{N} (u_i - E(u))(v_i - E(v)) \qquad (44)$$

where u and v denote the values of two adjacent samples in the original message signal or decrypted message signal and $E(u) = {}^1\!/_N \sum_{i=1}^{N} (u_i)$, $G(u) = {}^1\!/_N \sum_{i=1}^{N} (u_i - E(u))^2$, N signifies the number of samples involved in correlation calculation. The correlation distribution of two horizontally adjacent samples in the original and encrypted Boston satellite image are illustrated in Fig.13 (a) and Fig.13 (b), correspondingly. It is clear that the correlation coefficients of encrypted image are too small. It means that no detectable correlation exists among the original and its encrypted image. Thus, the suggested chaotic encryption algorithm has great security to statistical attacks.

- *Maximum and Irregular Deviation*

Maximum Deviation (MD) and Irregular Deviation (ID) measure the quality of encryption scheme. MD measures the quality of encryption scheme in the sense that how it maximizes the deviation between plaintext and ciphertext and ID measures how much the statistical distribution of histogram deviation is close to uniform distribution. MD is calculated as

$$MD = \frac{h_0 + h_{255}}{2} + \sum_{i=1}^{254} h_i \qquad (45)$$

where hi is the amplitude of the absolute difference curve between original and encrypted images at value i. Also,

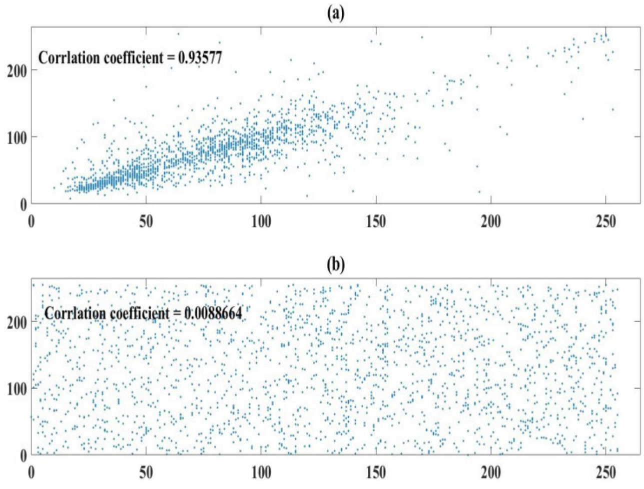


FIGURE 13. Correlations of two adjacent samples in the original image and the encrypted image.

to calculate ID, one can refer [51], [52].The computed values of MD and ID for different images are shown in TABLE 2 and TABLE 3, respectively.

TABLE 2. Encryption quality analysis of the scheme (MD).

Image	Encrypted Image	Encrypted Image [52]	Encrypted Image [53]
Boston	914262	-	-
Cameraman	63651	61812	64535

TABLE 3. Encryption quality analysis of the scheme (ID).

Image	Encrypted Image	Encrypted Image[52]	Encrypted Image [53]
Boston	691624	-	-
Cameraman	44158	40127	39250

- *Noise and Cropping Attack*

To test the performance of proposed encryption scheme in resisting noise attacks and data loss, the encrypted Boston satellite image was attacked by a 3% "salt & pepper" noise attack (Fig.14a) and a data cut with a size of 64 × 64 (Fig.15a), respectively. Then, these cipher images were decrypted and the results of the decryption are given in Fig.14b and Fig.15b, respectively. The results indicate that our scheme can resist cutting and noise pollution attacks. This is due to the fact that in the proposed method, the encryption process is done on the QAM symbols and the receiver can retrieve the original values of the QAM symbols by estimation methods such as optimum receiver.

- *Homogeneity, Energy and Contrast Analysis*

Homogeneity determines how closely the elements in the Gray-Level Co-occurrence Matrices (GLCM) are distributed to the GLCM diagonal. GLCM shows the statistical combinations of pixel grey levels in tabular form. The GLCM table

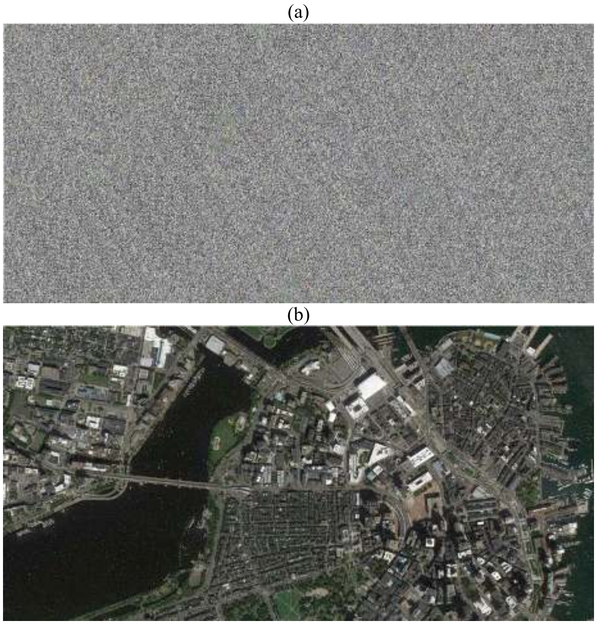


FIGURE 14. Noise attack. (a) the cipher image added with 3% "salt & pepper" noise (b) the decrypted image of (a).

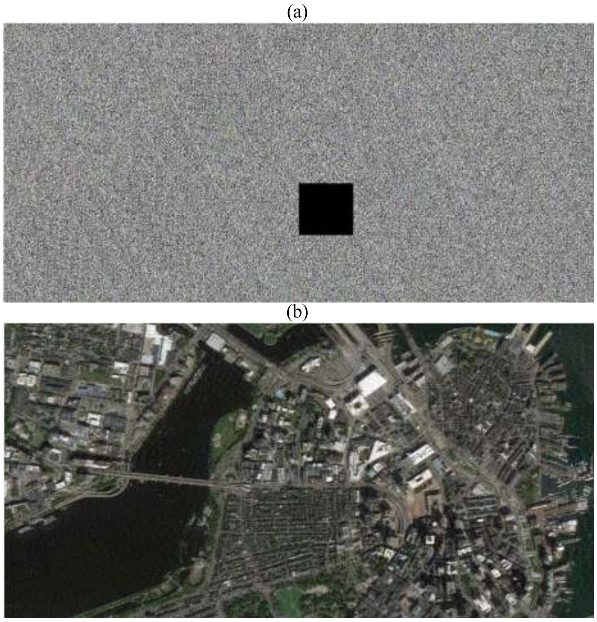


FIGURE 15. Cropping attack. (a) the cipher images with data loss; (b) the decrypted image of (a).

also determines the frequency of the patterns of different pixel gray levels. Mathematically, the homogeneity is defined as

$$Homogeneity = \sum_{i,j} \frac{p(i,j)}{1 + |\text{i-j}|} \tag{46}$$

where the gray-level co-occurrence matrices in GLCM is represented by $p(i, j)$. The computed values of homogeneity for different images are shown in TABLE 4. From TABLE 4, one can see the smaller values of homogeneity for the proposed satellite image encryption scheme. These smaller values of homogeneity reflect a higher secure nature of the proposed image encryption.

TABLE 4. **Homogeneity analysis.**

Image	Encrypted Image	Encrypted Image [53]
Boston	0.38981	-
Cameraman	0.38991	0.38827

Also, the energy is the statistical measurement of texture that considers the spatial relationship of pixels in the GLCM. Mathematically, the energy of a ciphertext image is given by

$$Energy = \sum_{i,j} p(i,j)^2 \tag{47}$$

where $p(i,j)$ represents the pixel value at index i and j. The energy values obtained for the proposed image encryption scheme are given in TABLE 5. The lower values of energy confirm a higher degree of disorder in the ciphertex image.

TABLE 5. **Energy analysis.**

Image	Encrypted Image	Encrypted Image [53]
Boston	0.015691	-
Cameraman	0.015638	0.015644

Moreover, the contrast analysis calculates the intensity differences between two neighboring pixels. Through contrast analysis, the viewer can clearly identify the object in texture of an image. Mathematically, the contrast is given by

$$Contrast = \sum_{i,j=1}^{N} p(i,j)\, |\text{i-j}|^2 \tag{48}$$

where $p(i,j)$ computes the number of GLCM matrices and N demonstrates the grand total of rows and columns. The values of contrast for the proposed scheme are shown in TABLE 6.

TABLE 6. **Contrast analysis.**

Image	Encrypted Image	Encrypted Image [53]
Boston	10.536	-
Cameraman	10.453	10.647

- *Classical types of attacks*

According to the Kerckhoffs principle, which is an important principle in cryptosystems, in evaluating the security of these systems, it should be assumed that attackers know exactly the design and working of the cryptosystem under study. According to this principle, the system security should not depend on the secrecy and confidentiality of its algorithms, but only depend on the confidentiality of cryptographic keys. Most modern cryptosystems are based on the Kirkhofs principle. As mentioned in [54], the classical attacks such as chosen plaintext attack, plaintext-only attack, chosen ciphertext attack, and ciphertext-only attack are most common attacks in cryptography. In these attacks, chosen plaintext is the most powerful attack and it can be said that if an encryption algorithm resists against the chosen plaintext attack, then it is resistant to other attacks. The proposed algorithm is sensitive to the system parameters α and η and the initial states $x_1(0)$, $x_2(0)$, $x_3(0)$ of the chaotic system. If one of the changes, the chaotic keys k_1, k_2 and k_3 would be totally different. Furthermore, in the chaotic constellation encryption, the output of the multi-shift cipher algorithm dependents on the parameter l in Eq.(37) which can be related to the former plain value and former ciphered value. This means that different ciphered images have different former plain values and former ciphered values. Hence, the proposed algorithm can resist the chosen plaintext/ ciphertext attack.

- *IE, NPCR and UACI metrics*

At last, in this subsection, the other useful metrics for image cryptosystem quality measurement such asIE, 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

$$IE(\phi) = \sum_{i=1}^{255} \hbar(\phi_i) \log(\frac{1}{\hbar(\phi_i)}) \tag{49}$$

where $\hbar(\phi_i)$ demonstrates the probability of variable ϕ_i and the entropy is calculated in bits. The information entropy value for a truly random source is equal to 8 [55]. 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 7.9986. It seems that the IE value of the suggested scheme is very close to 8.

Moreover, to measure the robustness of the encryption process to differential attacks, the NPCR and UACI values are used. 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 in one pixel of the original image at the position i, j and $\lambdabar(i,j)$ is a bipolar array which is defined as [56]

$$\lambdabar(i,j) = \begin{cases} 1 & if\ CI_1(i,j) \neq CI_2(i,j) \\ 0 & if\ CI_1(i,j) = CI_2(i,j) \end{cases} \tag{50}$$

Now, the NPCR and UACI quantities are calculated as

$$NPCR(CI_1, CI_2) = \sum_{i,j} \frac{\lambdabar(i,j)}{S} \times 100\% \tag{51}$$

$$UACI(CI_1, CI_2) = \sum_{i,j} \frac{|CI_1(i,j) - CI_2(i,j)|}{S.F} \times 100\% \tag{52}$$

where S represents the total number pixels in original image and F is the value of the largest theoreticalallowed value in encrypted image. The optimalvalues of NPCR and UACI are $NPCR_{opt} = 99.61\%$ and $UACI_{opt} = 33.46\%$, respectively [57]. The values of NPCR and UACI of suggested encryption method are 99.6159 and 34.3190, correspondingly. It is observed that NPCR and UACI are very close to the optimal values. In general, according to the practical results andperformance analysis, it is resulted that the suggested cryptosystem can hide the information of the satellite image perfectly.

VI. CONCLUSION

In this article, a chaotic secure communication technique is proposed for the encryption and secure transmission of satellite images through a channel with unknown time-delay propagation. In this regard, a robust controller is designed to synchronize the modified Chua oscillators at the transmitter and receiver with the time delay and parametric uncertainties in the finite time. A combination of chaotic keys and encryption method as multi-shift cipher encryption and chaotic masking of QAM symbols has been implemented to increase the security of the wireless OFDM. The purpose of this method is to remove all of the appearances of the original satellite imageduring the transmission, while protecting the quality of the recovered satellite image with an adequate level. Some of the features of the proposed approach are, 1) it incorporates the advantages of chaotic masking methods such as simplicity, low time consumption and very easily implementation in electronic circuits; 2) it eliminates the disadvantages of chaos masking such as weakness against conventional attack methods by using multi-shift cipher encryption algorithm and improving the security of masking method. The proposed approach was shown to be secure, reliable, robust and simple to implement. Moreover, the proposed cryptosystem exhibited acceptable resistance to different attacks. Finally, it is worth noting that the proposed chaos synchronization and encryption technique can be used with any conventional wireless/wired OFDM system.

REFERENCES

[1] G. Maral, M. Bousquet, and Z. Sun, *Satellite Communications Systems: Systems, Techniques and Technology*. Hoboken, NJ, USA: Wiley, 2020.

[2] E. M. Rogers and T. W. Valente, "A history of information theory in communication research," in *Between Communication and Information*. Abingdon, U.K.: Routledge, 2017, pp. 35–56.

[3] D. Renza, S. Mendoza, and D. M. Ballesteros, "High-uncertainty audio signal encryption based on the collatz conjecture," *J. Inf. Secur. Appl.*, vol. 46, pp. 62–69, Jun. 2019.

[4] S. Haddad, G. Coatrieux, A. Moreau-Gaudry, and M. Cozic, "Joint watermarking-encryption-JPEG-LS for medical image reliability control in encrypted and compressed domains," *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 2556–2569, 2020.

[5] L. Kocarev and S. Lian, *Chaos-Based Cryptography: Theory, Algorithms and Applications*. Cham, Switzerland: Springer, 2011.

[6] G.-D. Li and L.-L. Wang, "Double chaotic image encryption algorithm based on optimal sequence solution and fractional transform," *Vis. Comput.*, vol. 35, no. 9, pp. 1267–1277, Sep. 2019.

[7] T. Chuman, W. Sirichotedumrong, and H. Kiya, "Encryption-then-compression systems using grayscale-based image encryption for JPEG images," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 6, pp. 1515–1525, Jun. 2019.

[8] A. Alghafis, N. Munir, M. Khan, and I. Hussain, "An encryption scheme based on discrete quantum map and continuous chaotic system," *Int. J. Theor. Phys.*, vol. 59, no. 4, pp. 1227–1240, 2020.

[9] M. Jampour and A. Naserasadi, "Chaos game theory and its application for offline signature identification," *IET Biometrics*, vol. 8, no. 5, pp. 316–324, Sep. 2019.

[10] W. S. Sayed, M. F. Tolba, A. G. Radwan, and S. K. Abd-El-Hafiz, "FPGA realization of a speech encryption system based on a generalized modified chaotic transition map and bit permutation," *Multimedia Tools Appl.*, vol. 78, no. 12, pp. 16097–16127, 2019.

[11] H. Hermassi, M. Hamdi, R. Rhouma, and S. M. Belghith, "A joint encryption-compression codec for speech signals using the ITU-T G.711 standard and chaotic map," *Multimedia Tools Appl.*, vol. 76, no. 1, pp. 1177–1200, Jan. 2017.

[12] P. Sathiyamurthi and S. Ramakrishnan, "Speech encryption using chaotic shift keying for secured speech communication," *EURASIP J. Audio, Speech, Music Process.*, vol. 2017, no. 1, p. 20, Dec. 2017.

[13] H.-G. Chou, C.-F. Chuang, W.-J. Wang, and J.-C. Lin, "A fuzzy-model-based chaotic synchronization and its implementation on a secure communication system," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 12, pp. 2177–2185, Dec. 2013.

[14] X. Yi, R. Guo, and Y. Qi, "Stabilization of chaotic systems with both uncertainty and disturbance by the UDE-based control method," *IEEE Access*, vol. 8, pp. 62471–62477, 2020.

[15] Y. Niu, X. Zhang, and F. Han, "Image encryption algorithm based on hyperchaotic maps and nucleotide sequences database," *Comput. Intell. Neurosci.*, vol. 2017, pp. 1–9, Jan. 2017.

[16] J. Kalpana and P. Murali, "An improved color image encryption based on multiple DNA sequence operations with DNA synthetic image and chaos," *Optik*, vol. 126, no. 24, pp. 5703–5709, Dec. 2015.

[17] S. H. Strogatz, *Nonlinear Dynamics and Chaos With Student Solutions Manual: With Applications to Physics, Biology, Chemistry, and Engineering*. Boca Raton, FL, USA: CRC Press, 2018.

[18] J. Ma, A.-B. Li, Z.-S. Pu, L.-J. Yang, and Y.-Z. Wang, "A time-varying hyperchaotic system and its realization in circuit," *Nonlinear Dyn.*, vol. 62, no. 3, pp. 535–541, Nov. 2010.

[19] J. Ma, X. Wu, R. Chu, and L. Zhang, "Selection of multi-scroll attractors in jerk circuits and their verification using pspice," *Nonlinear Dyn.*, vol. 76, no. 4, pp. 1951–1962, Jun. 2014.

[20] Y. Zhang, "A new unified image encryption algorithm based on a lifting transformation and chaos," *Inf. Sci.*, vol. 547, pp. 307–327, Feb. 2021.

[21] R. A. D. Costa, M. B. Loiola, and M. Eisencraft, "Correlation and spectral properties of chaotic signals generated by a piecewise-linear map with multiple segments," *Signal Process.*, vol. 133, pp. 187–191, Apr. 2017.

[22] M. Eisencraft and D. M. Kato, "Spectral properties of chaotic signals with applications in communications," *Nonlinear Anal., Theory, Methods Appl.*, vol. 71, no. 12, pp. e2592–e2599, Dec. 2009.

[23] G. A. Al-Suhail, F. R. Tahir, M. H. Abd, V.-T. Pham, and L. Fortuna, "Modelling of long-wave chaotic radar system for anti-stealth applications," *Commun. Nonlinear Sci. Numer. Simul.*, vol. 57, pp. 80–96, Apr. 2018.

[24] S. Hu, L. Wang, J. Mao, C. Gao, B. Zhang, and S. Yang, "Synchronous online diagnosis of multiple cable intermittent faults based on chaotic spread spectrum sequence," *IEEE Trans. Ind. Electron.*, vol. 66, no. 4, pp. 3217–3226, Apr. 2019.

[25] B. Vaseghi, M. A. Pourmina, and S. Mobayen, "Finite-time chaos synchronization and its application in wireless sensor networks," *Trans. Inst. Meas. Control*, vol. 40, no. 13, pp. 3788–3799, Sep. 2018.

[26] M. Herceg, D. Vranješ, R. Grbić, and J. Job, "Chaos-based transmitted-reference ultra-wideband communications," *Int. J. Electron.*, vol. 106, no. 1, pp. 160–172, Jan. 2019.

[27] M. Preishuber, T. Hutter, S. Katzenbeisser, and A. Uhl, "Depreciating motivation and empirical security analysis of chaos-based image and video encryption," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 9, pp. 2137–2150, Sep. 2018.

[28] J. S. Khan and J. Ahmad, "Chaos based efficient selective image encryption," *Multidimensional Syst. Signal Process.*, vol. 30, no. 2, pp. 943–961, Apr. 2019.

[29] Y. Naseer, D. Shah, and T. Shah, "A novel approach to improve multimedia security utilizing 3D mixed chaotic map," *Microprocessors Microsyst.*, vol. 65, pp. 1–6, Mar. 2019.

[30] Y. Zhang, "The fast image encryption algorithm based on lifting scheme and chaos," *Inf. Sci.*, vol. 520, pp. 177–194, May 2020.

[31] T. Wu, C. Zhang, H. Huang, Z. Zhang, H. Wei, H. Wen, and K. Qiu, "Security improvement for OFDM-PON via DNA extension code and chaotic systems," *IEEE Access*, vol. 8, pp. 75119–75126, 2020.

[32] L. M. Pecora and T. L. Carroll, "Synchronization in chaotic systems," *Phys. Rev. Lett.*, vol. 64, no. 8, p. 821, 1990.

[33] B. Vaseghi, M. A. Pourmina, and S. Mobayen, "Secure communication in wireless sensor networks based on chaos synchronization using adaptive sliding mode control," *Nonlinear Dyn.*, vol. 89, no. 3, pp. 1689–1704, Aug. 2017.

[34] T.-H. Chien and Y.-C. Chen, "Combination of observer/Kalman filter identification and digital redesign of observer-based tracker for stochastic chaotic systems," in *Proc. Int. Symp. Comput., Consum. Control (ISC)*, Jul. 2016, pp. 103–107.

[35] H. Zhang, D. Meng, J. Wang, and G. Lu, "Synchronisation of uncertain chaotic systems via fuzzy-regulated adaptive optimal control approach," *Int. J. Syst. Sci.*, vol. 51, no. 3, pp. 473–487, Feb. 2020.

[36] B. Liu, Z. Sun, Y. Luo, and Y. Zhong, "Uniform synchronization for chaotic dynamical systems via event-triggered impulsive control," *Phys. A, Stat. Mech. Appl.*, vol. 531, Oct. 2019, Art. no. 121725.

[37] X. Lu, "A financial chaotic system control method based on intermittent controller," *Math. Problems Eng.*, vol. 2020, pp. 1–12, Mar. 2020.

[38] S. Singh and A. T. Azar, "Multi-switching combination synchronization of fractional order chaotic systems," in *Proc. Joint Eur.-US Workshop Appl. Invariance Comput. Vis.* Cham, Switzerland: Springer, 2020, pp. 655–664.

[39] S. Mobayen and J. Ma, "Robust finite-time composite nonlinear feedback control for synchronization of uncertain chaotic systems with nonlinearity and time-delay," *Chaos, Solitons Fractals*, vol. 114, pp. 46–54, Sep. 2018.

[40] M. A. Khelifa and A. Boukabou, "Design of an intelligent prediction-based neural network controller for multi-scroll chaotic systems," *Int. J. Speech Technol.*, vol. 45, no. 3, pp. 793–807, Oct. 2016.

[41] M. Zapateiro De la Hoz, L. Acho, and Y. Vidal, "A modified chua chaotic oscillator and its application to secure communications," *Appl. Math. Comput.*, vol. 247, pp. 712–722, Nov. 2014.

[42] Y. Hong, G. Yang, L. Bushnell, and H. O. Wang, "Global finite-time stabilization: From state feedback to output feedback," in *Proc. 39th IEEE Conf. Decis. Control*, vol. 3, Dec. 2000, pp. 2908–2913.

[43] H. Wang, J.-P. Wu, X.-S. Sheng, X. Wang, and P. Zan, "A new stability result for nonlinear cascade time-delay system and its application in chaos control," *Nonlinear Dyn.*, vol. 80, nos. 1–2, pp. 221–226, Apr. 2015.

[44] Y. Tang, "Terminal sliding mode control for rigid robots," *Automatica*, vol. 34, no. 1, pp. 51–56, Jan. 1998.

[45] R. V. Nee and R. Prasad, *OFDM for Wireless Multimedia Communications*. Norwood, MA, USA: Artech House, 2000.

[46] K. Fallahi, R. Raoufi, and H. Khoshbin, "An application of chen system for secure chaotic communication based on extended Kalman filter and multi-shift cipher algorithm," *Commun. Nonlinear Sci. Numer. Simul.*, vol. 13, no. 4, pp. 763–781, Jul. 2008.

[47] J. S. Khan, J. Ahmad, and M. A. Khan, "TD-ERCS map-based confusion and diffusion of autocorrelated data," *Nonlinear Dyn.*, vol. 87, no. 1, pp. 93–107, Jan. 2017.

[48] S. F. Abbasi, J. Ahmad, J. S. Khan, M. A. Khan, and S. A. Sheikh, "Visual meaningful encryption scheme using intertwinning logistic map," in *Proc. Sci. Inf. Conf.* Cham, Switzerland: Springer, 2018, pp. 764–773.

[49] X. Fu, M. Bi, X. Zhou, G. Yang, Q. Li, Z. Zhou, and X. Yang, "A chaotic modified-DFT encryption scheme for physical layer security and PAPR reduction in OFDM-PON," *Opt. Fiber Technol.*, vol. 42, pp. 126–131, May 2018.

[50] J. S. Khan, W. Boulila, J. Ahmad, S. Rubaiee, A. U. Rehman, R. Alroobaea, and W. J. Buchanan, "DNA and plaintext dependent chaotic visual selective image encryption," *IEEE Access*, vol. 8, pp. 159732–159744, 2020.

[51] F. A. Khan, J. Ahmed, J. S. Khan, J. Ahmad, and M. A. Khan, "A novel image encryption based on lorenz equation, gingerbreadman chaotic map and s8 permutation," *J. Intell. Fuzzy Syst.*, vol. 33, no. 6, pp. 3753–3765, Nov. 2017.

[52] J. Ahmad, M. A. Khan, F. Ahmed, and J. S. Khan, "A novel image encryption scheme based on orthogonal matrix, skew tent map, and XOR operation," *Neural Comput. Appl.*, vol. 30, no. 12, pp. 3847–3857, Dec. 2018.

[53] S. Zhu and C. Zhu, "Plaintext-related image encryption algorithm based on block structure and five-dimensional chaotic map," *IEEE Access*, vol. 7, pp. 147106–147118, 2019.

[54] X. Wang, L. Teng, and X. Qin, "A novel colour image encryption algorithm based on chaos," *Signal Process.*, vol. 92, no. 4, pp. 1101–1108, Apr. 2012.

[55] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, vol. 28, no. 4, pp. 656–715, Oct. 1949.

[56] J. S. Khan, J. Ahmad, S. F. Abbasi, and S. K. Kayhan, "DNA sequence based medical image encryption scheme," in *Proc. 10th Comput. Sci. Electron. Eng. (CEEC)*, Sep. 2018, pp. 24–29.

[57] Y. Wu, J. P. Noonan, and S. Agaian, "NPCR and UACI randomness tests for image encryption cyber journals: Multidisciplinary journals in science and technology," *J. Sel. Areas Telecommun.*, vol. 1, no. 2, pp. 31–38, 2011.

BEHROUZ VASEGHI was born in Esfahan, Iran, in 1981. He received the B.Sc. and M.Sc. degrees in electrical engineering from Islamic Azad University (IAU), Najafabad Branch, Esfahan, in 2004 and 2008, respectively, and 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 with 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.

SEYEDEH SOMAYEH HASHEMI was born in Zanjan, Iran, in 1982. She received the B.Sc. and M.Sc. degree in electrical engineering from Islamic Azad University (IAU), Naeen Branch, Esfahan, Iran, in 2004 and 2008, respectively, and the Ph.D. degree in communication engineering from IAU, Science and Research Branch, Tehran, Iran, in 2020. Since 2009, she has been a full-time member with the Department of Electrical Engineering, IAU, Abhar Branch. Since 2020, she has been an Assistant Professor with the Department of Electrical Engineering, IAU, Abhar Branch. Her research interests include communication systems, audio and video processing, chaotic systems, chaotic cryptography, and chaos synchronization.

SALEH MOBAYEN (Member, IEEE) received the B.Sc. and M.Sc. degrees in control engineering from the University of Tabriz, Tabriz, Iran, in 2007 and 2009, respectively, and the Ph.D. degree in control engineering from Tarbiat Modares University, Tehran, Iran, in January 2013. From February 2013 to December 2018, he was an Assistant Professor and a Faculty Member with the Department of Electrical Engineering, University of Zanjan, Zanjan, Iran. Since December 2018, he has been an Associate Professor of Control Engineering with the Department of Electrical Engineering, University of Zanjan. He currently collaborates with the National Yunlin University of Science and Technology as an Associate Professor with the Future Technology Research Center. He has published several articles in the national and international journals. His research interests include control theory, sliding mode control, robust tracking, non-holonomic robots, and chaotic systems. He is a member of the IEEE Control Systems Society and program committee of several international conferences. He is an Associate Editor of *Artificial Intelligence Review*, *International Journal of Control, Automation and Systems*, *Circuits, Systems, and Signal Processing*, *Journal of Simulation*, *Measurement and Control*, *Complexity*, and *International Journal of Dynamics and Control*, an Academic Editor of *Mathematical Problems in Engineering*, and an Associate Editor of *SN Applied Sciences* and other international journals.

AFEF FEKIH (Senior Member, IEEE) received the B.S., M.S., and Ph.D. degrees in electrical engineering from the National Engineering School of Tunis, Tunisia, in 1995, 1998, and 2002, respectively. She is currently a Full Professor with the Department of Electrical and Computer Engineering and the Chevron/BORSF Professor of Engineering with the University of Louisiana at Lafayette. Her research interests include 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. She is a member of the IEEE Control Systems Society, the IEEE Women in Control Society, and the IEEE Industrial Electronics Society.