IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received January 10, 2021, accepted January 27, 2021, date of publication February 1, 2021, date of current version February 16, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3056037

Fast Reaching Finite Time synchronization Approach for Chaotic Systems With Application in Medical Image Encryption

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

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

Corresponding authors: Behrouz Vaseghi (behrouz.vaseghi@gmail.com) and Saleh Mobayen (mobayens@yuntech.edu.tw)

ABSTRACT This article proposes a fast reaching finite time synchronization approach for chaotic systems along with its application to medical image encryption. First, an adaptive terminal sliding mode tracking approach with fast reaching condition is designed to synchronize the chaotic systems at the transmitter and receiver ends in finite time. Then, a chaotic cryptosystem, using synchronized chaotic systems as secret keys generator, is proposed to enhance the security of medical image transmission and/or storage. The applicability and efficiency of the proposed synchronization approach is assessed using a simulation as well as an analytical study. The analysis encompassed security tools such as histogram analysis, correlation test, and information entropy change the rate of the number of pixels and unified average changing intensity. The obtained results confirmed the robustness and fast convergence rate of the proposed synchronization approach. The security analysis also shows that the proposed cryptosystem displays acceptable levels of resistance to various attacks.

INDEX TERMS Chaos synchronization, fast reaching condition, medical image encryption, MORE method encryption.

I. INTRODUCTION

Chaos theory is a branch of mathematics that studies nonlinear complex systems exhibiting high sensitivities [1]–[4]. The issue of chaotic synchronization was described for the first time by Afraimovich *et al.* [5] and later developed by Ott, Grebogi and York [6]. Notwithstanding all the work which has been done by the mathematicians on chaos theory and synchronization, it is only the recent event done by Carroll and Pecora [7] on chaos synchronization that attracted a lot of attention to the application of chaos in engineering sciences. Carroll and Pecora have demonstrated, experimentally and theoretically, that if the chaotic system is modeled using a master-slave structure, then the two chaotic signals can be synchronized. In terms of chaos synchronization techniques, various approaches have been proposed in the literature. For instance, sliding mode control [8], digital redesign control [9], optimal control [10], backstepping method [11], impulsive control [12], intermittent scheme [13], switching process [14], composite nonlinear feedback [10], fuzzy-logic control [15] and neural-based control [16] have been considered. Sliding mode control (SMC) is an effective robust control technique which has been used for the synchronization or control of chaos in power electronic systems [17], [18], touchless fingerprint encryption [19], satellite motion [20], cryptosystem [21], wind speed forecasting [22], Van der Pol oscillator [23], wind power interval prediction [24], nonlinear pendulum [25], image encryption [26], secure communication [27], [28] and so on. Among the attractive features of SMC are its robustness to uncertainties, fast response, computational simplicity and insensitivity to disturbances [18], [29]–[33].

The rapid development of electronic technology has led to their widespread adoption in hospitals, notably in picture archiving and communication systems [34]. These latter enable the storage of patients' diagnostic results in the form of digital images. These images often contain sensitive data such as patients' personal information [35]. Consequently,

The associate editor coordinating the review of this manuscript and approving it for publication was Choon Ki Ahn.

safeguarding the storage and transfer of this information is crucial to protecting patients' privacy. Though, conventional encryption schemes are able to satisfy the security of multimedia information during transmission, there are still some limitations when it comes to protecting all multimedia content and preventing illegal access. Research has shown that these methods, in some cases, have exhibited defects against brute-force attacks due to lower key space. Additionally, in most cases, traditional encryption methods require high computing power and long computational time. In real-time applications, such as wireless communication due to the low speed of encryption and decryption, they may present considerable latency. In this context, cryptography using chaotic signals offers a set of promising techniques which can exhibit some advantages over the traditional encryption techniques, especially in terms of a good combination of security, speed and capability. Encryption methods using chaotic systems is an encryption technology which uses synchronized chaotic signals generated by chaotic systems to create keys in encryption systems. These chaotic keys have good features such as large key space and are extremely sensitive to the system parameters and initial conditions [36], [37]. Because of the high security and low cost of chaotic signals and the attractive features of SMC, the implementation of a medical image encryption using an SMC-based synchronized chaotic system is an attractive solution that can perfectly resolve the security issues in safe medical communication systems.

This paper designs and implements a fast reaching technique finite time synchronization technique for chaotic systems with application in medical image encryption. Its main contributions are threefold:

- An adaptive terminal sliding mode tracking approach based on a novel sliding manifold with fast reaching condition to synchronize chaotic systems at the transmitter and receiver ends in finite time.
- A synchronization approach that can practically be implemented to the chaotic systems without the need for any unrealistic assumptions about the knowledge of the upper bounds of the external disturbances.
- A chaotic cryptosystem using a synchronized chaotic system as secret key generator to enhance the security of the medical image transmission and/or storage.

This paper is organized as follows. Section 2 provides some definitions and preliminaries. The Main results, including the sliding surface design, finite time control, fast reaching condition and adaptive control approach are detailed in section 3. The proposed chaotic cryptosystem including the chaotic key-stream generation, random number generation algorithms and medical image encryption and decryption schemes are explained in section 4. The simulation results are presented in section 5. The performance analyses including the statistical analysis are provided in section 6. Finally, some concluding remarks are given in section 7.

II. SYSTEM DEFINITION AND PRELIMINARIES

Consider the following canonical description of a chaotic system with external disturbances:

$$\begin{aligned}\dot{x}_1(t) &= x_2(t)\\ \dot{x}_2(t) &= x_3(t)\\ \dot{x}_3(t) &= f(x(t),t) + b(x(t),t)\,u(t) + d(x(t),t)\end{aligned} \quad (1)$$

where $x(t) = [x_1(t), x_2(t), x_3(t)]^T$ are the system states, $u(t)$ is the control input, $b(x(t),t)$ and $f(x(t),t)$ are two nonlinear functions with known bounds, and $d(x(t),t)$ indicates the external disturbance with $|d(x(t),t)| \leq \delta$, where δ is a positive scalar. The control objective is to force the nonlinear disturbed system (1) to track the reference trajectories defined by:

$$\begin{aligned}\dot{x}_{1d}(t) &= x_{2d}\\ \dot{x}_{2d}(t) &= x_{3d}\\ \dot{x}_{3d}(t) &= g(x_d(t),t)\end{aligned} \quad (2)$$

where $g(x_d(t),t)$ is a differentiable function of time.

Define the tracking error signals as

$$e(t) = x_1(t) - x_{1d}(t) \quad (3)$$

$$\dot{e}(t) = x_2(t) - x_{2d}(t) \quad (4)$$

$$\ddot{e}(t) = x_3(t) - x_{3d}(t) \quad (5)$$

In what follows, we propose a terminal sliding mode approach to ensure the finite-time convergence of the tracking errors to the origin.

III. MAIN RESULTS

A. SLIDING SURFACE DESIGN

Define the following terminal sliding mode control surface:

$$s(e(t)) = \ddot{e}(t) + \varsigma\dot{e}(t) + \lambda e(t) + \mu e(t)^{\eta} \quad (6)$$

where $\lambda, \mu, \varsigma > 0$ and $1 > \eta > 0$ is a ratio of two odd positive integers. Using (1)-(6), the time-derivative of $s(e(t))$ is obtained as

$$\begin{aligned}\dot{s}(e(t)) &= e(t) + \varsigma\ddot{e}(t) + \lambda\dot{e}(t) + \mu\dot{e}(t)e(t)^{\eta-1}\\ &= \dot{x}_3(t) - \dot{x}_{3d}(t) + \varsigma(x_3(t) - x_{3d}(t))\\ &\quad +\lambda(x_2(t) - x_{2d}(t)) + \mu(x_2(t)\\ &\quad -x_{2d}(t))e(t)^{\eta-1}\\ &= f(x(t),t) + b(x(t),t)u(t) + d(x(t),t)\\ &\quad -\dot{x}_{3d}(t) + \varsigma(x_3(t) - x_{3d}(t))\\ &\quad + \left(\lambda + \mu e(t)^{\eta-1}\right)(x_2(t) - x_{2d}(t))\end{aligned} \quad (7)$$

B. FINITE TIME CONTROL

In the subsequent theorem, the finite time convergence of the fast terminal sliding surface based on the fast reaching condition is satisfied. In this section, it is shown that the fast reaching condition drives the error trajectories to converge to the sliding surface with a fast speed. After the convergence of the tracking errors to the sliding surface, the tracking objective of the reference trajectory is fulfilled.

Theorem 1: Consider the nonlinear disturbed system (1) and assume that the external disturbance $d(x(t),t)$ is bounded by a positive constant δ. The terminal sliding mode tracker with the fast reaching condition is designed as:

$$\begin{aligned} u(t) = & -b(x(t),t)^{-1}(f(x(t),t) - \dot{x}_{3d}(t) \\ & +\varsigma(x_3(t) - x_{3d}(t)) \\ & +\left(\lambda + \mu e(t)^{\eta-1}\right)(x_2(t) - x_{2d}(t)) \\ & +m_1\left(\beta^{|s(e(t))|} - 1\right) sgn(s(e(t))) \\ & +m_2 |s(e(t))|^{\alpha} sgn(s(e(t))) \\ & +\delta sgn(s(e(t)))) \end{aligned} \tag{8}$$

where $m_1, m_2 > 0$, $0 < \alpha < 1$ and $\beta = 1 + m_2/m_1$. Then, the sliding surface converges to the origin in finite time and the reachability condition of the terminal sliding surface (6) is satisfied.

Proof: Construct the Lyapunov function as:

$$V(s) = 0.5 s(e(t))^2 \tag{9}$$

where differentiating (9) with respect to time and using (7), yields:

$$\begin{aligned} \dot{V}(s) = & s(e(t))(f(x(t),t) + b(x(t),t)u(t) \\ & +d(x(t),t) - \dot{x}_{3d}(t) + \varsigma(x_3(t) - x_{3d}(t)) \\ & +(\lambda + \mu e(t)^{\eta-1})(x_2(t) - x_{2d}(t))) \end{aligned} \tag{10}$$

Substituting (8) into (10), gives

$$\begin{aligned} \dot{V}(s) = & s(e(t))(d(x(t),t) - m_1\left(\beta^{|s(e(t))|} - 1\right) sgn(s(e(t))) \\ & -m_2 |s(e(t))|^{\alpha} sgn(s(e(t))) - \delta sgn(s(e(t)))), \end{aligned} \tag{11}$$

where, since $|d(x(t),t)| \leq \delta$, Eq. (11) gives

$$\begin{aligned} \dot{V}(s) = & d(x(t),t)\, s(e(t)) - m_2 |s(e(t))|^{\alpha+1} \\ & -m_1\left(\beta^{|s(e(t))|} - 1\right)|s(e(t))| - \delta |s(e(t))| \\ \leq & (|d(x(t),t)| - \delta)|s(e(t))| \\ & -m_1\left(\beta^{|s(e(t))|} - 1\right)|s(e(t))|\, m_2 |s(e(t))|^{\alpha+1} \\ \leq & -m_1\left(\beta^{|s(e(t))|} - 1\right)|s(e(t))| \\ & -m_2 |s(e(t))|^{\alpha+1} \end{aligned} \tag{12}$$

According to the Lyapunov function (9), one obtains $|s(e(t))| = \sqrt{2}\, V(s)^{\frac{1}{2}}$. Since $m_1, m_2 > 0$ and $\gamma = \beta^{|s(e(t))|} - 1 \geq 0$, Eq. (12) can be rewritten as

$$\dot{V}(s) \leq -\sqrt{2} m_1 \gamma V(s)^{\frac{1}{2}} - 2^{\frac{\alpha+1}{2}} m_2 V(s)^{\frac{\alpha+1}{2}} < 0 \tag{13}$$

The last condition means that the terminal sliding mode surface (6) based on the fast reaching condition converges to the origin in the finite time.

C. FAST REACHING CONDITION

In the terminal sliding mode control law (8), two important terms have been used, i.e., $-m_1\left(\beta^{|s(e(t))|} - 1\right) sgn(s(e(t)))$ and $-m_2 |s(e(t))|^{\alpha} sgn(s(e(t)))$. By combining these two terms, the fast reaching condition is formed as:

$$\begin{aligned} \dot{s}(e(t)) = & -m_1\left(\beta^{|s(e(t))|} - 1\right) sgn(s(e(t))) \\ & -m_2 |s(e(t))|^{\alpha} sgn(s(e(t))) \end{aligned} \tag{14}$$

When the tracking errors are far away from the switching surface ($|s(e(t))| > 1$), the first term of (14) has a dominant task. In this condition, the change rate of the first term is larger than that of the second term of $\dot{s}(e(t))$ and it speeds up the reaching rate. In addition, when the tracking errors are near to the surface ($|s(e(t))| < 1$), the second term of (14) plays the dominant role. The combination of the effects of two terms in $\dot{s}(e(t))$ can force the tracking system to have a superior dynamic performance.

When the initial value of the sliding surface ($s(e(0))$) is greater than one ($s(e(0)) > 1$), the process of motion from the initial value to the sliding mode is divided into two phases:

(*a*): $s(e(0)) \rightarrow s(e(t)) = 1$. In this phase, one can obtain $s(e(t)) > 1$; then $m_1(\beta^{|s(e(t))|} - 1) > m_2 |s(e(t))^{\alpha}|$, and the second term of (14) is ignored. Hence, the reaching condition (14) is simplified as

$$\dot{s}(e(t)) \approx -m_1(\beta^{s(e(t))} - 1) \tag{15}$$

where integrating both sides of (15) yields:

$$\int_0^{t_a} dt \approx -\frac{1}{m_1 \ln\beta} \int_{s(e(0))}^{1} d(\ln(1 - \beta^{-s(e(t))})) \tag{16}$$

Then, the tracking convergence time of phase a ($s(e(0)) \rightarrow s(e(t)) = 1$) is found as

$$t_a \approx \frac{\ln\left(1 - \beta^{-s(e(0))}\right) - \ln(1 - \beta^{-1})}{m_1 \ln\beta} \tag{17}$$

(*b*): $s(e(t)) = 1 \rightarrow s(e(t)) = 0$ In this phase, we have $m_1(\beta^{|s(e(t))|} - 1) < m_2 |s(e(t))^{\alpha}|$; the second term of (14) has a prominent duty and the first term is ignored. Therefore, the reaching condition (14) can be simplified as

$$\dot{s}(e(t)) \approx -m_2 s(e(t))^{\alpha} \tag{18}$$

where by integrating Eq. (18), we have:

$$\int_0^{t_b} dt \approx -\frac{1}{m_2} \int_1^0 \frac{ds}{s(e(t))^{\alpha}} \tag{19}$$

The tracking convergence time of phase b ($s(e(t)) = 1 \rightarrow s(e(t)) = 0$) is calculated as

$$t_b \approx \frac{1}{m_2(1 - \alpha)} \tag{20}$$

Hence, the total convergence time is the combination of the times (17) and (20) as

$$t_{total} \approx t_a + t_b = \frac{\ln\left(1 - \beta^{-s(e(0))}\right) - \ln\left(1 - \beta^{-1}\right)}{m_1 \ln\beta}$$

$$+\frac{1}{m_2(1-\alpha)} \tag{21}$$

When the initial value of the sliding surface is smaller than -1, i.e., $s(e(0)) < -1$, the process of motion from the initial value to the sliding mode is divided into the following two phases:

(*c*): $s(e(0)) \rightarrow s(e(t)) = -1$. In this phase, we have $s(e(t)) < -1$; then $m_1(\beta^{|s(e(t))|} - 1) > m_2 |s(e(t))^{\alpha}|$, the first term of (14) has a prevailing effect and the second term is ignored. Thus, the reaching condition (14) is written as

$$\dot{s}(e(t)) \approx m_1(\beta^{-s(e(t))} - 1 \tag{22}$$

where by integrating (22), it follows

$$\int_0^{t_c} dt \approx -\frac{1}{m_1 \ln \beta} \int_{s(e(0))}^{-1} d(\ln(1 - \beta^{-s(e(t))})) \tag{23}$$

Then, the convergence time of phase $c(s(e(0)) \rightarrow s(e(t)) = -1)$ is calculated as

$$t_c \approx \frac{\ln\left(1 - \beta^{-s(e(0))}\right) - \ln(1 - \beta^{-1})}{m_1 \ln \beta} \tag{24}$$

$(d)s(e(t)) = -1 \rightarrow s(e(t)) = 0$. In this phase, one can obtain $m_1(\beta^{|s(e(t))|} - 1) < m_2 |s(e(t))^{\alpha}|$; the second term of (14) plays a dominant role and the first term is ignored. The reaching condition (14) is converted to

$$\dot{s}(e(t)) \approx -m_2(-s(e(t)))^{\alpha} \tag{25}$$

where integrating (25) yields

$$\int_0^{t_d} dt \approx \frac{1}{m_2} \int_{-1}^{0} \frac{ds}{(-s(e(t)))^{\alpha}} \tag{26}$$

The convergence time of phase $d(s(e(t)) = -1 \rightarrow s(e(t)) = 0)$ is obtained as

$$t_d \approx \frac{1}{m_2(1-\alpha)} \tag{27}$$

The total convergence time can be found from (24) and (27) as:

$$t_{total} \approx t_c + t_d = \frac{\ln\left(1 - \beta^{s(e(0))}\right) - \ln\left(1 - \beta^{-1}\right)}{m_1 \ln \beta} + \frac{1}{m_2(1-\alpha)} \tag{28}$$

As a result, the error trajectories, in both conditions $|s(e(t))| > 1$ and $|s(e(t))| < -1$, converge to the terminal sliding surface in finite time. On the sliding surface $(s(e(t)) = 0)$, in the light of Eq. (14), the time-derivative of the sliding surface is zero, i.e. $\dot{s}(e(t)) = 0$. It means that the velocity at which the error trajectories reach the sliding surface is equal to zero. This case reduces the chattering phenomenon efficiently.

D. ADAPTIVE CONTROL APPROACH

In real applications, it is impossible to determine the upper bound of the external disturbances $d(x(t), t)$. To solve this problem, an estimation of the positive constant δ, i.e. $\hat{\delta}(t)$, is suggested in the following theorem.

Theorem 2: Consider the nonlinear disturbed system (1) and the terminal sliding surface (6). Assume that the external disturbance $d(x(t),t)$ is bounded by a positive unknown constant δ, which is estimated by $\hat{\delta}(t)$. The adaptive terminal sliding mode tracking controller with the fast reaching condition is designed as

$$\begin{aligned} u(t) = & -b(x(t), t)^{-1}(f(x(t), t) - \dot{x}_{3d}(t) + \varsigma(x_3(t) \\ & -x_{3d}(t)) + \left(\lambda + \mu e(t)^{\eta-1}\right)(x_2(t) - x_{2d}(t)) \\ & +m_1\left(\beta^{|s(e(t))|} - 1\right) sgn(s(e(t))) \\ & +m_2 |s(e(t))|^{\alpha} sgn(s(e(t))) \\ & +\hat{\delta}(t) sgn(s(e(t)))) \end{aligned} \tag{29}$$

and the estimation law is given by

$$\dot{\hat{\delta}}(t) = l^{-1} |s(e(t))| \tag{30}$$

where l is a positive constant. Then, the reachability condition of the terminal sliding surface (6) is guaranteed.

Proof: Assume the estimation error as

$$\tilde{\delta}(t) = \hat{\delta}(t) - \delta \tag{31}$$

Using (30) and (31), the time-derivative of $\tilde{\delta}(t)$ is found as

$$\dot{\tilde{\delta}}(t) = \dot{\hat{\delta}}(t) = l^{-1} |s(e(t))| \tag{32}$$

Consider the positive-definite Lyapunov function as

$$V(s, \tilde{\delta}) = 0.5\left\{s(e(t))^2 + l\tilde{\delta}(t)^2\right\} \tag{33}$$

where differentiating the Lyapunov function and using (7) and (32), we have

$$\begin{aligned} \dot{V}(s, \tilde{\delta}) &= s(e(t))\dot{s}(e(t)) + l\tilde{\delta}(t)\dot{\tilde{\delta}}(t) \\ &= \tilde{\delta}(t) |s(e(t))| \\ &\quad +s(e(t))(f(x(t), t) + b(x(t), t)u(t) \\ &\quad +d(x(t), t) - \dot{x}_{3d}(t) + \varsigma(x_3(t) - x_{3d}(t)) \\ &\quad +(\lambda + \mu e(t)^{\eta-1})(x_2(t) - x_{2d}(t))). \end{aligned} \tag{34}$$

Now, substituting (29) into (34), one attains:

$$\begin{aligned} \dot{V}(s, \tilde{\delta}) = & \tilde{\delta}(t) |s(e(t))| + s(e(t))(d(x(t), t) \\ & -(\hat{\delta}(t) + m_2 |s(e(t))|^{\alpha} \\ & +m_1(\beta^{|s(e(t))|} - 1)) sgn(s(e(t)))). \end{aligned} \tag{35}$$

Since $s(e(t))d(x(t), t) \leq |s(e(t))| |d(x(t), t)|$ and $|s| = s.sgn(s)$, Eq. (35) can be written as

$$\begin{aligned} \dot{V}(s, \tilde{\delta}) \leq & \tilde{\delta}(t) |s(e(t))| + |s(e(t))| |d(x(t), t)| \\ & -\hat{\delta}(t) |s(e(t))| - m_2 |s(e(t))|^{\alpha+1} \\ & -m_1\left(\beta^{|s(e(t))|} - 1\right) |s(e(t))|. \end{aligned} \tag{36}$$

By addition and subtraction of the term $\delta(t)\,|s(e(t))|$ to the right-hand-side of (36), we have

$$\begin{aligned}\dot{V}(s,\tilde{\delta}) \leq & \left(\hat{\delta}(t)-\delta(t)\right)|s(e(t))| \\ & +|s(e(t))|\,|d(x(t),t)|-\hat{\delta}(t)\,|s(e(t))| \\ & -m_2\,|s(e(t))|^{\alpha+1} \\ & -m_1\left(\beta^{|s(e(t))|}-1\right)|s(e(t))| \\ & +\delta(t)\,|s(e(t))|-\delta(t)\,|s(e(t))|\,, \end{aligned} \tag{37}$$

where simplifying Eq. (37) gives

$$\begin{aligned}\dot{V}(s,\tilde{\delta}) \leq & -m_1\left(\beta^{|s(e(t))|}-1\right)|s(e(t))| \\ & -m_2\,|s(e(t))|^{\alpha+1} \\ & -(\delta(t)-|d(x(t),t)|)\,|s(e(t))| \\ \leq & -m_1\left(\beta^{|s(e(t))|}-1\right)|s(e(t))| \\ & -m_2\,|s(e(t))|^{\alpha+1}\,. \end{aligned} \tag{38}$$

Hence, according to the estimation-based tracking control law (29), it is resulted that the Lyapunov function (33) decreases gradually, i.e., $\dot{V}(s,\tilde{\delta}) \leq 0$. This finalizes the proof.

Remark 1. There is tradeoff between the controller's complexity and its performance. However, in this paper, due to the usage of synchronized chaotic system to implementation of the information cryptosystem, the more complexity of the controller causes more complexity of the cryptosystem. In fact, if the eavesdropper wants to extract the original data from the encrypted data, he/she will face more complexity to achieve the encryption keys and the security performance will improve. Therefore, it can be concluded that in the chaotic cryptography applications, the consideration of the cryptographic performance can take precedence over the control performance.

IV. PROPOSED MEDICAL IMAGE ENCRYPTION

The block diagram of the proposed medical image encryption system is illustrated in Fig.1. In this system, the reference trajectories (2) considered as the transmitter chaotic system and the equation (1) considered as the receiver chaotic system. Note that the focus of our work is on the proposed chaotic encryption and decryption approach. The details about the wireless multimedia communication system can be found in [38].

A. CHAOTIC KEY AND RANDOM BIT GENERATION

At first, the parameters and initial states of the transmitter chaotic system are defined. Then, the sampling interval of the system (Δh) is determined and the chaotic system is solved using the fourth-order Runge–Kutta (RK-4) integration algorithm. As a result of the system analysis, three chaotic signals as 15 digit float values $[x_{1d}(i), x_{2d}(i), x_{3d}(i)]$ are obtained. By using the chaotic sequences $x_{1d}(i), x_{2d}(i)$ and $x_{3d}(i)$, the chaotic keys (ck) are generated as follow:

$$\begin{aligned} ck1(i) &= \mathrm{mod}(x_{1d}\,(i)\,, floor(x_{1d}(i-1))) \\ ck2(i) &= \mathrm{mod}(x_{2d}\,(i)\,, floor(x_{2d}(i-1))) \\ ck3(i) &= \mathrm{mod}(x_{3d}\,(i)\,, floor(x_{3d}(i-1))) \end{aligned} \tag{39}$$

where the function mod (f, g) returns the remainder of f divided by g, and $floor(\omega)$ rounds the elements of ω to the nearest integers. Also, on the chaotic float values $x_{1d}(i), x_{2d}(i)$ and $x_{3d}(i)$ obtained from step 1, the values of the decimal parts after the comma(fraction part) are considered. These values are converted to 64 bit binary digits and 32 LSBs with low-valued and high-precision (rb_x, rb_y, rb_z). This process is done to generate 1 million bits per phase. Following the generation of these random bits for each phase, the phases are subjected to XOR processing in binary form. The new random bit sequences are generated by

$$\begin{aligned} rb_{xy} &= bitxor(rb_x, rb_y) \\ rb_{xz} &= bitxor(rb_x, rb_z) \\ rb_{yz} &= bitxor(rb_y, rb_z) \\ rb_{xyz} &= bitxor(rb_x, rb_y, rb_z) \end{aligned} \tag{40}$$

At last, the final random bits (rb) are obtained as

$$rb = [rb_{xy}, rb_{xz}, rb_{yz}, rb_{xyz}] \tag{41}$$

B. MEDICAL IMAGE ENCRYPTION

After obtaining the chaotic keys $[ck1, ck2, ck3]$ and random bits $[rb]$, in this subsection, a medical image P measuring $m \times n$ was used for encryption by combination of Chaotic Matrix Operation for Randomization or Encryption (C-MORE) method and XOR operation. Conventional MORE Method as a probabilistic symmetrical fully homomorphic cryptosystem was fully described in [39], [40]. The details of the encryption are explained as follow:

Step1: Convert the medical image P into a vector $\tilde{P}$ of length $m \times n$.

Step 2: For each sample pixel of the image vector $\tilde{P}(j)$, the invertible matrix $S(j)$ is formed using the chaotic keystream $(ck1)$ as

$$S(j) = \begin{bmatrix} s_{11} & s_{12} \\ s_{21} & s_{22} \end{bmatrix} = \begin{bmatrix} ck1(4j-3) & ck1(4j-2) \\ ck1(4j-1) & ck1(4j) \end{bmatrix} \tag{42}$$

By using the matrix $S(j)$ and chaotic key streams $(ck2)$ and $(ck3)$, the pixel value $\tilde{P}(j)$ is encrypted by

$$C(j) = \begin{bmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \end{bmatrix} = S(j) \begin{bmatrix} ck2\,(j)\,.\tilde{P}(j) & 0 \\ 0 & ck3(j) \end{bmatrix} S(j)^{-1} \tag{43}$$

where $c_{11}, c_{12}, c_{21}, c_{22}$ are four encrypted pixel values related to one pixel value of the original image vector $\tilde{P}(j)$. This process is done for all of the pixels $(\tilde{P}(j)\,|j = 1, 2, \ldots, m \times n)$ and the encrypted values are gathered to build four encrypted pixel vectors $[C_1, C_2, C_3, C_4]$.

Step 3: For more security, the encrypted pixels vector $[C_1, C_2, C_3, C_4]$ are encrypted again with random bit sequences obtained from (41) by XOR operation as

$$\tilde{E}_k = C_k \oplus rn, k = 1, \ldots, 4 \tag{44}$$

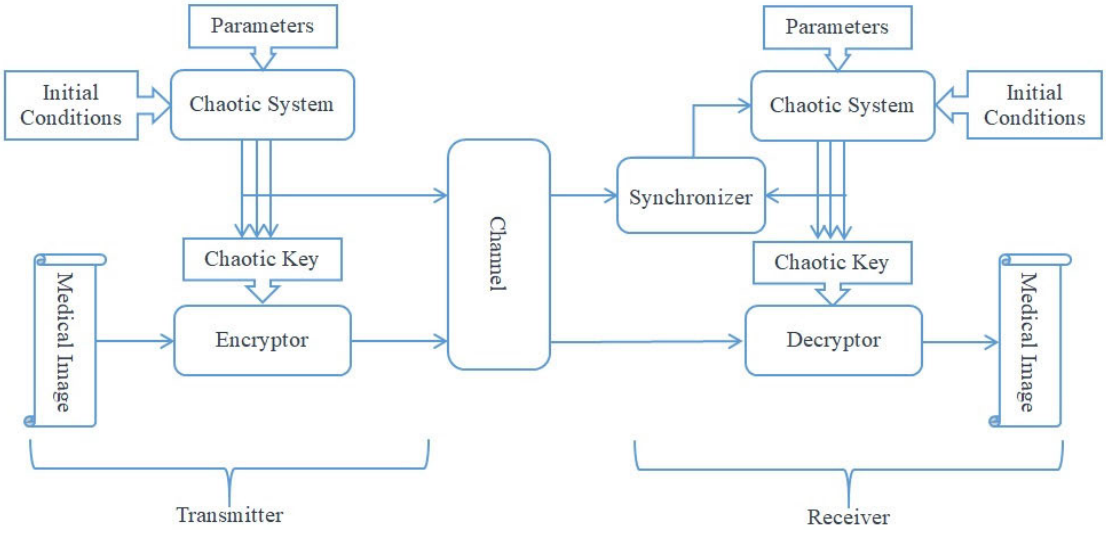

FIGURE 1. Block diagram of the proposed chaotic encryption-decryption system.

Finally, four encrypted images related to the original medical image can be obtained by reshaping the encrypted vectors $\left[\tilde{E}_1, \tilde{E}_2, \tilde{E}_3, \tilde{E}_4\right]$ to the four matrixes $[E_1, E_2, E_3, E_4]$ of size $m \times n$. These four encrypted images are sent to the receiver using a TX/RX module through a public noisy wireless channel which can be accessed by an eavesdropper.

C. MEDICAL IMAGE DECRYPTION

When the synchronization process described in Sec. III is achieved and the chaotic signals at the receiver end are synchronized with the chaotic signals at the transmitter, the original medical image can be recovered by applying the reverse operations in the encryption as follow:

Step 1: Using the initial states, system parameters and control inputs of the receiver chaotic system, the chaotic synchronization is achieved and the chaotic key streams $[ck1, ck2, ck3]$ and random bits $[rb]$ are obtained at the receiver with the same process of Sec. IV-A.

Step 2: Four encrypted images $[E_1, E_2, E_3, E_4]$ related to the original medical image that received at the receiver, convert into four vectors $\left[\tilde{E}_1, \tilde{E}_2, \tilde{E}_3, \tilde{E}_4\right]$. By using the random numbers $[rb]$ and XOR operation, one can obtain

$$C'_k = \tilde{E}_k \oplus rb, k = 1, \ldots, 4 \tag{45}$$

Step 3: By using the chaotic key stream $(ck1)$, the invertible matrix $S'(j)$ can be reconstructed for each cipher-texts sample pixel $[C'_1(j), C'_2(j), C'_3(j), C'_4(j)]$ in the receiver as

$$S'(j) = \begin{bmatrix} s'_{11} & s'_{12} \\ s'_{21} & s'_{22} \end{bmatrix} = \begin{bmatrix} ck1(4j-3) & ck1(4j-2) \\ ck1(4j-1) & ck1(4j) \end{bmatrix} \tag{46}$$

Now, the sample value $\tilde{P}'(j)$ can be recovered by chaotic key streams $ck2$ and $ck3$ as

$$D(j) = \begin{bmatrix} d_{11} & d_{12} \\ d_{21} & d_{22} \end{bmatrix} = S'(j)^{-1} \begin{bmatrix} C'_1(j) & C'_2(j) \\ C'_3(j) & C'_4(j) \end{bmatrix} S'(j)$$

$$= \begin{bmatrix} ck2(j).\tilde{P}'(j) & 0 \\ 0 & ck3(j) \end{bmatrix} \tag{47}$$

Finally, by selecting the first array $ck2\,(j)\,.\tilde{P}'(j)$ of the matrix $D(j)$ and removing the weight $ck2\,(j)$, the plain-text sample pixel $\tilde{P}'(j)$ is obtained. This process is done for all of the cipher-text sample pixels $[C'_k\,(j)\,, k = 1, \ldots, 4, j = 1, 2, \ldots, m \times n]$ and by reshaping the recovered vector $\tilde{P}'$ to the matrix P' of size $m \times n$ the original medical image P' is recovered.

Remark 2. In this study, we have focused on medical image encryption because of the heightened security concerns about patients' privacy and the need for a robust and secure encryption method for such images. Moreover, we found that various methods such as the approach of [41] are effective for the general image. The medical images mainly contain the few colors and low details. Hence, these methods are not suitable for the medical image, and realizing the encryption take much time. Figure 2 shows the encryption result for medical image encryption by the method of [41]. Nonetheless, the proposed approach can be broadly implemented to other types of images.

V. SIMULATION RESULTS

A. SIMULATION RESULTS OF CHAOS SYNCHRONIZATION

The performance and robustness of the proposed fast reaching finite time synchronization approach is illustrated in this section using a numerical simulation study. In this simulation, the reference trajectories (2) as the transmitter chaotic system is considered with the condition $[x_{1d}\,(0)\,, x_{2d}\,(0)\,, x_{3d}\,(0)] = [0, 0, 0]$ and differentiable function

$$g(x_d(t), t) = -|x_{1d}(t)| - x_{2d}(t) + 0.6x_{3d}(t) + 1 \tag{48}$$

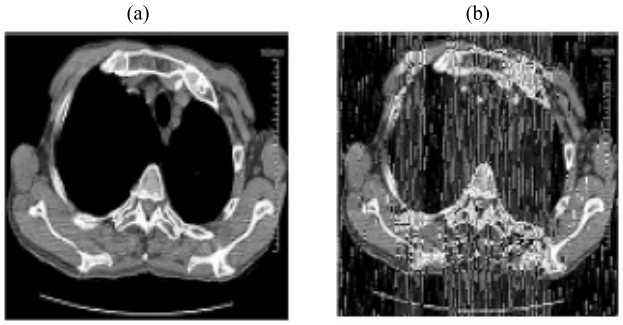

FIGURE 2. (a) Original image (b) encryption result by the method in [41].

The receiver chaotic system(1) is specified with initial condition $[x_1(0), x_2(0), x_3(0)] = [1, 1, 1]$ and system parameters:

$$f(x(t), t) = -|x_1(t)| - x_2(t) + 0.6x_3(t) + 1 \quad (49)$$

$$b(x(t), t) = 0.5\sin(x_1(t)) + \cos(x_2(t)) + 1.2\sin(x_3(t)) \quad (50)$$

$$d(x(t), t) = 0.2\sin(x_1(t) * t) + \cos(x_2(t) * t) + 0.15\sin(x_3(t) * \sqrt{t}) \quad (51)$$

The state trajectories of the chaotic systems are illustrated in Figs. 3-5, when the suggested controller (29) is applied. It is seen that the chaotic signals $x_1(t)$ and $x_{1d}(t)$ are synchronized in 5 seconds. Also, the state trajectories $x_2(t)$ and $x_3(t)$ are synchronized with $x_{2d}(t)$ and $x_{3d}(t)$ in 4 and 2 seconds, respectively. Fig.6 displays the dynamics of the error signals. It is shown from Fig.6 that the error signals converge to zero in less than 5 seconds. Thus, it can be concluded that the proposed method is able to mitigate the parametric uncertainties while displaying a suitable synchronization performance. The time responses of the designed control inputs $u(t)$ and FTSM surface $s(t)$ are shown in Fig.7. Note from the figure that the acceptable amplitudes of the proposed control law and FTSM surface. Note also the dynamics of the control signal and FTSM surface are free of chattering.

B. SIMULATION RESULTS ILLUSTRATING THE MEDICAL IMAGE ENCRYPTION SYSTEM

In this subsection, the usefulness and application of proposed scheme for medical image encryption is validated using numerical simulation. A medical skull image of size $444 \times 535 \times 3$ uint8, in JPG format is used in this simulation as the original data which must be encrypted (see Fig.8). The encryption keys are generated by the transmitter chaotic system. By applying these chaotic keys and the encryption method described in subsection IV-B, the original image is encrypted. Fig.9 shows the obtained encrypted images. At the receiver side, the chaotic system is used to generate the decryption keys. The decrypted medical skull image can be obtained after the synchronization procedure and the decryption process illustrated in Fig.10. From these figures, it can be seen that the encrypted images have uniform distribution, and the encrypted images are similar to the noise. It demonstrates that from the viewpoint of visual impression, the proposed method has a well encryption performance.

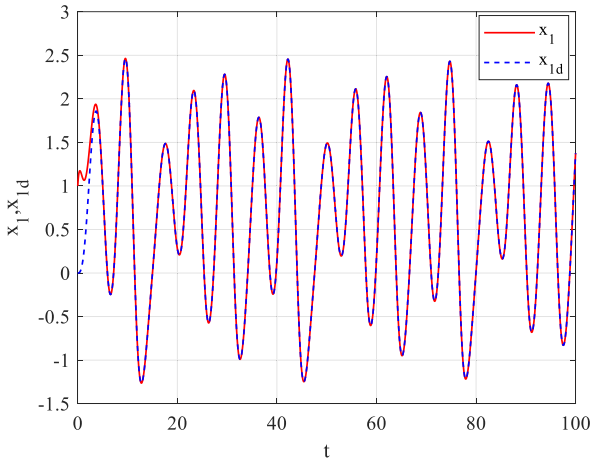

FIGURE 3. State trajectories x_1, x_{1d}.

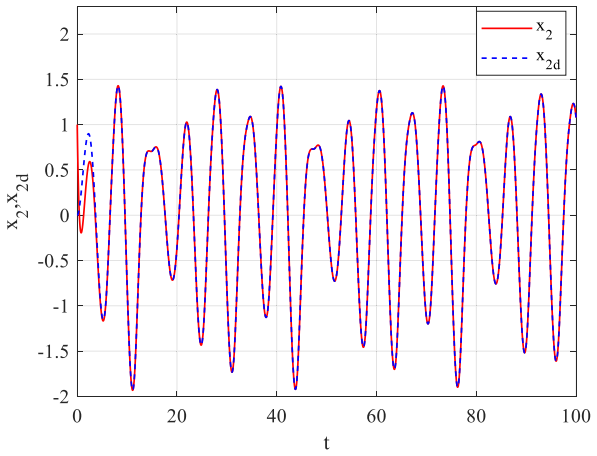

FIGURE 4. State trajectories x_2, x_{2d}.

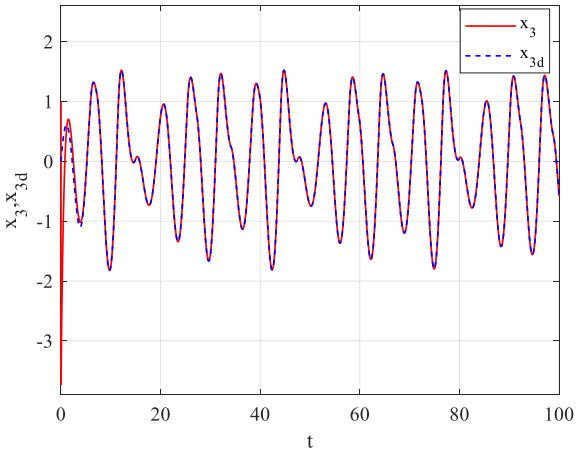

FIGURE 5. State trajectories x_3, x_{3d}.

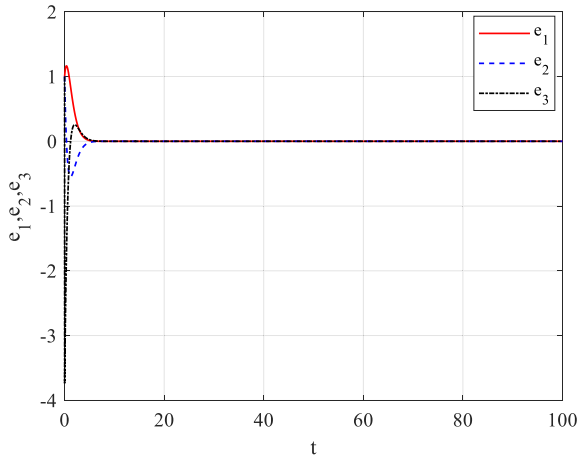

FIGURE 6. Error signals e_1, e_2, e_3.

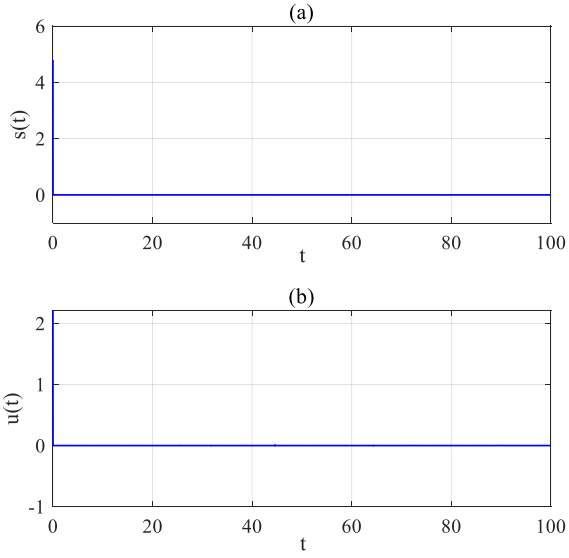

FIGURE 7. FTSM surface $s(t)$ and control signal $u(t)$.

FIGURE 8. Original skull image.

Remark 3. In the finite time control, the convergence time is dependent to the initial conditions. Although any finite-time convergent sliding mode controller can be transformed into a fixed-time convergent control approach [42]; however, for the application of synchronized chaotic systems in data encryption, because the output of the chaotic system is extremely sensitive to the initial conditions, the transmitter can obtain the new encryption keys by the change of the initial conditions. On the other hand, when the synchronization process is achieved in a new time and the chaotic signals at the receiver are synchronized with the chaotic signals at the transmitter, the new encryption keys and the original data can be recovered respectively.

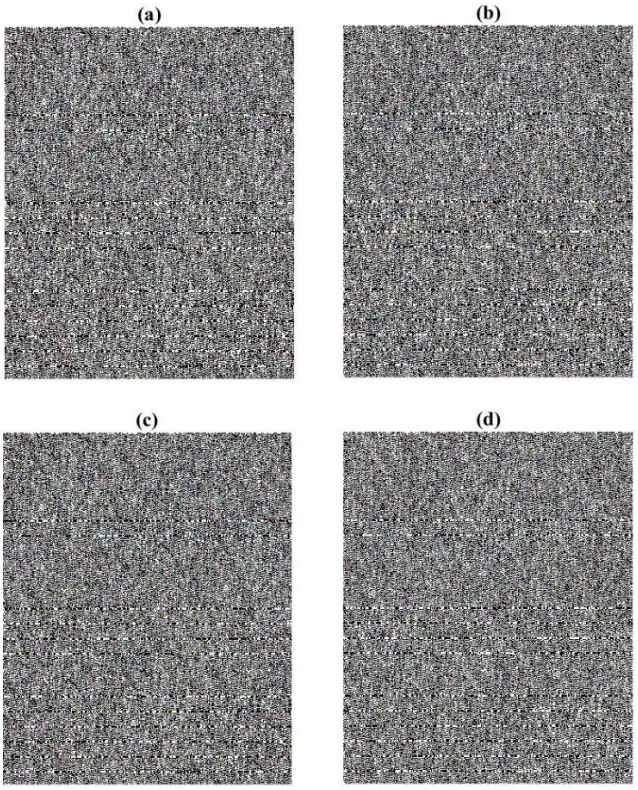

FIGURE 9. Encrypted skull images.

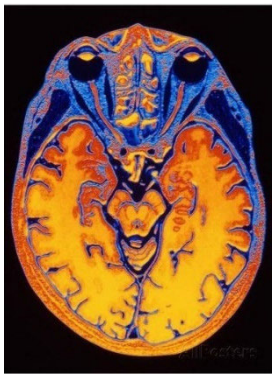

FIGURE 10. Recovered skull image.

Remark 4. The finite time convergence in synchronization of the chaotic systems has a very important role and significance for the realization of synchronization and secure communication. Since the finite time convergence can fulfill

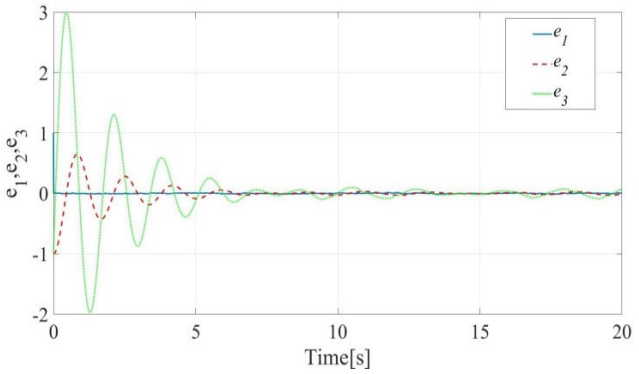

FIGURE 11. Synchronization errors using the controller in [45].

the identification of the system parameters in finite time, it can be ensured that the encoding of the original signal is completed in a given finite time that is shorter than the signal duration [43]. Moreover, in the data communication networks such as wireless sensor networks, there are many restrictions, including restrictions on battery lifetime. Thus, reduction of the synchronization time causes the sensors return to the idle mode more fast and consequently, the battery lifetime is increased [44]. Fig.11 shows the time trajectories of the synchronization errors using the method of [45]. As can be observed in this figure, the asymptotic convergence is achieved in more than 10 seconds. It can be expected that some errors might occur initially in the transient responses during the message decryption. In order to avoid this problem, the authors have proposed that the dummy information are sent in the beginning of the communication so as to prevent the loss of information, while the total time for communication is less than the considered time.

VI. PERFORMANCE ANALYSIS OF THE PROPOSED CRYPTOSYSTEM

To analyze the robustness and illustrate the adequate security of the proposed chaotic cryptosystem, we perform in this section a set of security analysis tests. That is, histogram analysis, correlation test, analysis of occlusion and noise attack, classical attack, information entropy, number of pixels change rate and unified average changing intensity are carried out. Additionally, to have a fair judgment and to further compare our approach to other works, we consider a classical standard test image (Lena) of size 512×512 uint 8. The results of the encryption process for the Lena image are illustrated in figures. 12-14.

A. HISTOGRAM ANALYSIS

To barricade the revelation of image information from an eavesdropper, it is useful if the encrypted image has no or very few statistical similarities to the original image. The histogram of image illustrated that pixel elements in an image are distributed using graphical display of the pixel elements, by measuring the color intensity level of each pixel element. The histograms of the original and encrypted medical skull

FIGURE 12. Original Lena image.

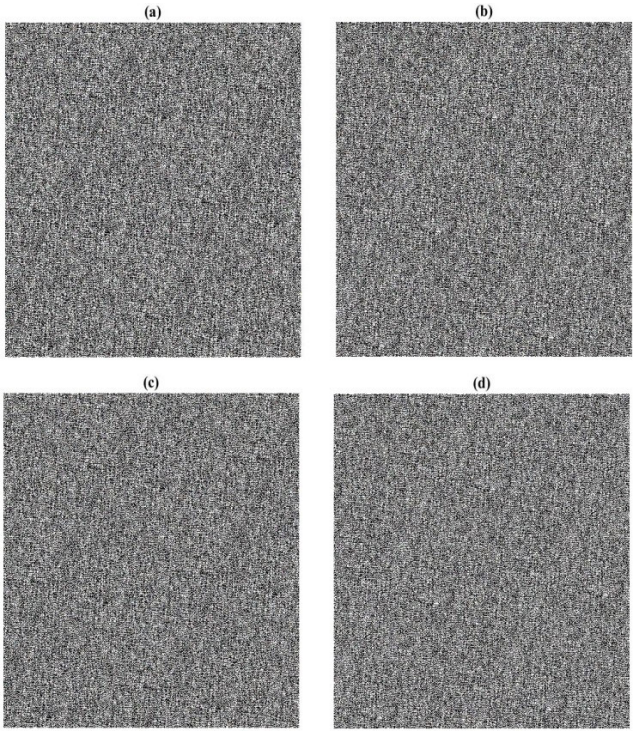

FIGURE 13. Encrypted Lena images.

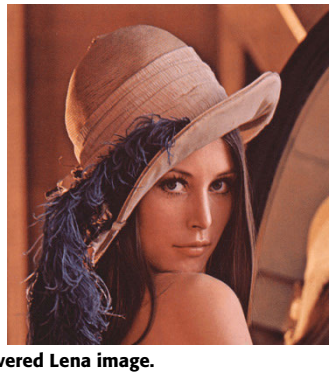

FIGURE 14. Recovered Lena image.

image are shown in Fig.15. The histograms of the encrypted images are more uniform, considerably different from the original image and have no statistical similarity to the original

TABLE 1. Variance of histogram.

Image	Original Image	Encrypted Image	Encrypted Image [46]
skull image	272842.3075	1418.78	-
Lena image	632097.4766	3309.2581	3485.1953

TABLE 2. Correlation coefficients of two adjacent pixels.

Image	Original Image	Encrypted Image	Encrypted Image [46]
skull image	0.96771	0.003932	-
Lena image	0.91281	0.002151	0.001412

image. Therefore, the encrypted medical skull images successfully hide the information of the original medical skull image.

Moreover, the variance of a histogram can quantitatively describe the distribution of pixel values, which is calculated by [46]:

$$var(Z) = \frac{1}{n^2} \sum_{i=1}^{n-1} \sum_{j=1}^{n-1} \frac{1}{2} \left(z_i - z_j\right)^2 \tag{52}$$

where Z is a vector and $Z = \{z_1, z_2, \ldots, z_{256}\}$, 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 medical skull image, Lena image and their encrypted images are calculated by using Equation (52) 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.

B. CORRELATION TEST

Pearson's correlation, developed by mathematician Karl Pearson and made public knowledge in 1884 can be used in correlation coefficient tests that will measure or compute the degree of similarity between two variables [47]. According to the Pearson's correlation, a good way to measure the encryption quality of an encryption system is by calculating the correlation coefficient between two adjacent sample values in the original message or the encrypted message. This metric can be calculated by [48]:

$$Corr\,(u, v) = \frac{cov\,(u, v)}{\sqrt{G\,(u)}\sqrt{G\,(v)}} \tag{53}$$

$$Cov\,(u, v) = {}^{1}\!/_{N} \sum\nolimits_{i=1}^{N} (u_i - E(u))(v_i - E(v)) \tag{54}$$

where u and v are the values of two adjacent samples in the original message signal or decrypted message signal and $E\,(u) = N^{-1} \sum_{i=1}^{N} u_i$, $G\,(u) = N^{-1} \sum_{i=1}^{N} (u_i - E(u))^2$, N represents the number of samples involved in the correlation calculation. The correlation distribution of two horizontally adjacent samples in the original and encrypted medical skull images are illustrated in Fig.16. Also, the mean absolute value of the correlation coefficients for medical skull image and Lena image have been given in Table 2 and compared with reference [46]. It is clear that the correlation coefficients of the encrypted images are too small. It means that no detectable correlation exists among the original and its corresponding encrypted images. Thus, the suggested chaotic encryption algorithm has great security against statistical attacks.

C. ANALYSIS OF OCCLUSION AND NOISE ATTACK

Encrypted images are subject to occlusion or cropping attack during transmission and may be partially damaged. Nevertheless, digital images allow a certain extent of distortion on the transmission channel. An ideal cryptosystem should against data loss attacks by transmission and storage. Also, in practical applications, noise interference is inevitable which can be due to thehigh bit error rate. An outstanding encryption algorithm has the ability to resist noise attack. To test the performance of proposed encryption scheme in resisting data loss, the encrypted medical skull images were attacked by a data cut with size of 64×64 as shown in Fig.17 (a-d). The result of the decryption is given in Fig.18. As can be seen from the decrypted figure, the original medical skull image recovered with some noise distortion and blurring and it can still be recognized with the details.

Moreover, to evaluate the robustness of the proposed encryption algorithm against the noise attack, the encrypted medical skull images were attacked with the 3% "salt & pepper" noise attack (see Fig.19). Then, these encrypted images were decrypted and the result of the decryption is given in Fig.20. It can be said from this figure that our algorithm has good robustness and can efficiently resist noise attacks.

D. CLASSICAL TYPES OF ATTACK

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 [49], 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 and the initial states of the chaotic

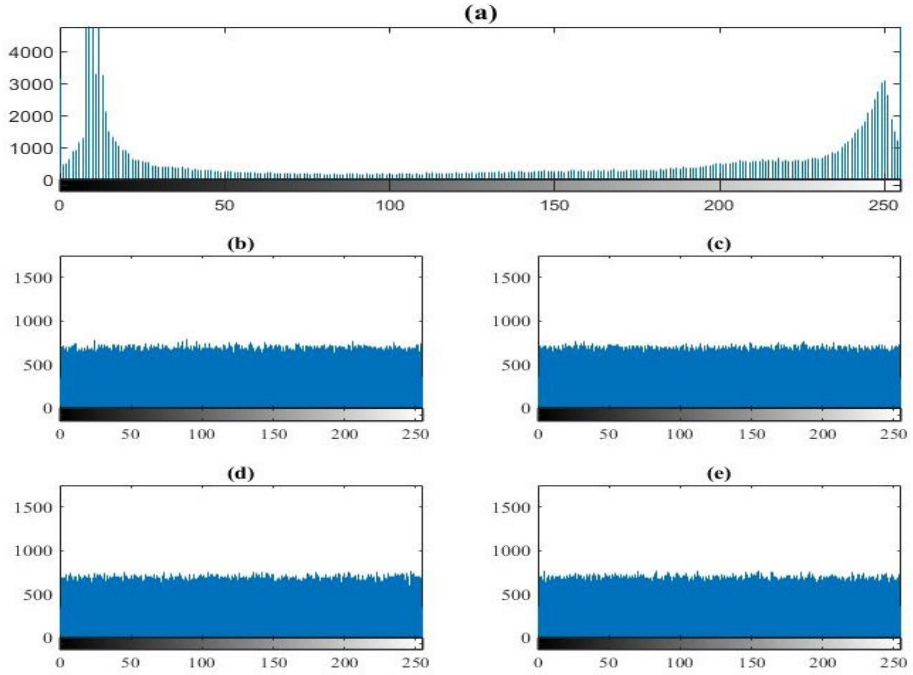

FIGURE 15. Histograms of (a) original image, (b, c, d, e) encrypted images.

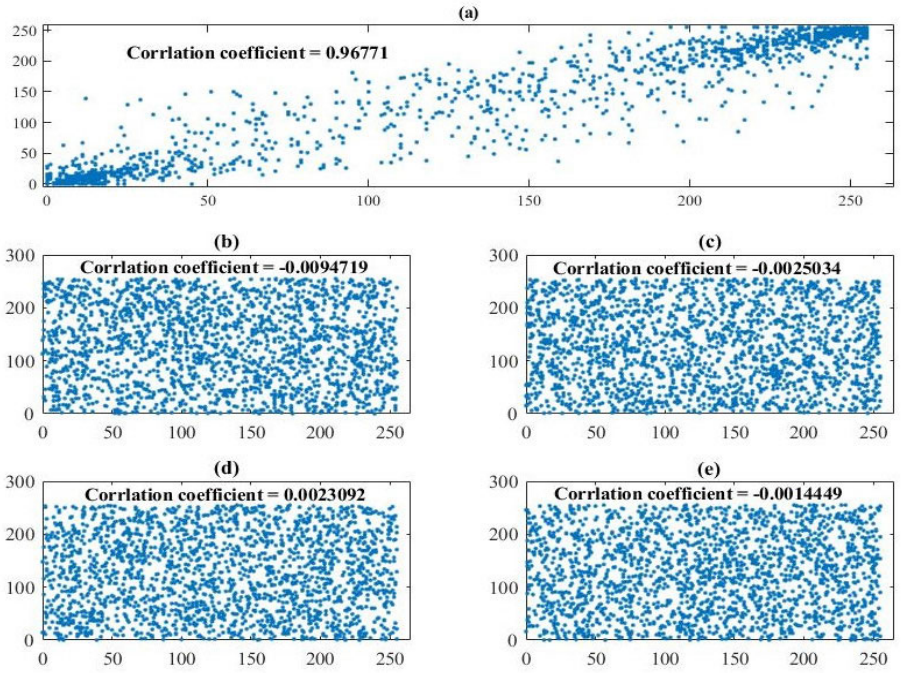

FIGURE 16. Correlations of two adjacent samples in (a) original image, (b, c, d, e) encrypted images.

system. If one of them changes, the chaotic keyswould be totally different. Furthermore, in the proposed chaotic MORE encryption, different chaotic keys are used to encrypt each pixel of the image. 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.

E. IE, NPCR AND UACI METRICS

Additional image cryptosystem quality measurement metrics such asInformation entropy (IE), Number of Pixels Change Rate (NPCR) and unified average Changing intensity (UACI) are considered in this section.

In information entropy theory, the complexity of the encrypted data is determined by calculating the information

TABLE 3. IE, NPCR and UACI metrics.

Image	IE	NPCR	UACI
skull image	7.9224	99.62	33.61
Lena image	7.9982	99.98	33.51
Lena image[46]	7.9990	99.99	33.40

entropy for an image as follows [50]:

$$IE\ (m) = \sum_{i=1}^{255} p(m_i)\log(\frac{1}{p(m_i)}) \tag{55}$$

where $p(m_i)$ represents the probability of variable m_i and the entropy is calculated in bits. The information entropy value for a truly random source is equal to 8 [48]. The closer the information entropy is to the quantity of 8, the better the quality of the encryption. The IE value of the proposed encryption method is 7.9224. Thus, the obtained IE value of the proposed method is very close to 8.

The number of pixels change rate (NPCR) and unified averagechanging intensity (UACI) are two metrics that are used to measure the strength of theencryption process to differential attacks. For our best knowledge, NPCR and UACI are first shown in 2004 [51]. In fact; the rate of changes 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 C_1 and C_2 are two encrypted images after and before changing in the one pixel of the original image at the position i, j and $d\ (i, j)$ is a bipolar array which is defined as

$$d\ (i,j) = \begin{cases} 1 & if\ C_1(i,j) \neq C_2(i,j) \\ 0 & if\ C_1(i,j) = C_2(i,j) \end{cases} \tag{56}$$

Now, the NPCR and UACI quantities are calculated as [52]

$$NPCR\ (C_1, C_2) = \sum_{i,j} \frac{d(i,j)}{S} \times 100\% \tag{57}$$

$$UACI\ (C_1, C_2) = \sum_{i,j} \frac{|C_1\ (i,j) - C_2\ (i,j)|}{S.F} \times 100\% \tag{58}$$

where S denotes the total number pixels in the original image and F is the value of the largest theoreticalallowed value in encrypted image. The optimalvalues of the NPCR and UACI are $NPCR_{opt}= 99.61\%NPCR_{opt}= 99.61\%$ and $UACI_{opt}= 33.46\%UACI_{opt}= 33.46\%$, respectively [52]. The values of NPCR and UACI of our suggested encryption method are 99.6281 and 33.6120, correspondingly. It is observed that NPCR and UACI are very close to the optimal values. Additionally, the IE, NPCR and UACI metrics were given for both the medical skull image and the Lena image in Table 3 and compared with reference [46]. In conclusion, we can deduct from the practical results and performance analysis, that the suggested cryptosystem can perfectly hide the information of the medical image.

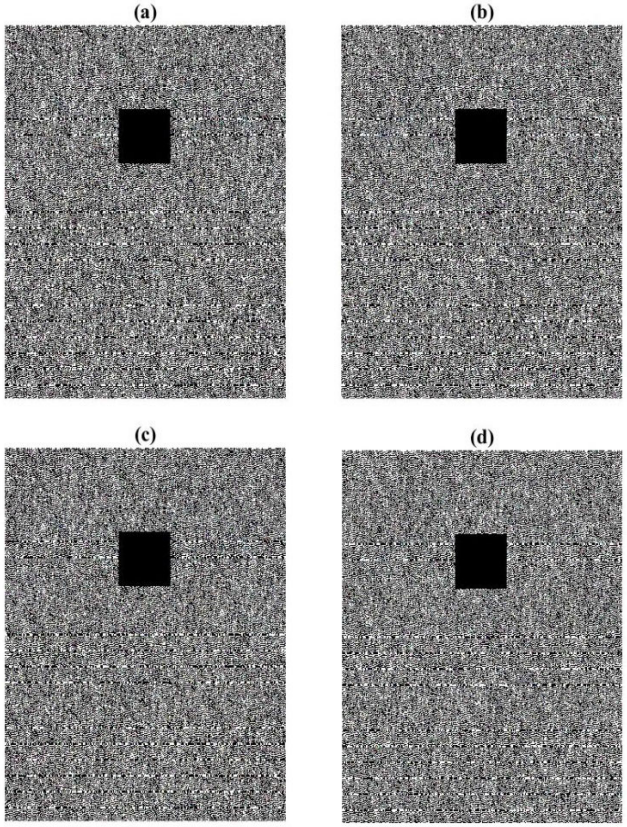

FIGURE 17. The encrypted images with data loss.

F. TIME ANALYSIS

A practical encryption algorithm should be efficient in terms of security and encryption time. The simulation experiments were run on a PC with Intel(R) Core(TM) i7-6820HQ CPU @ 2.70GHz, 16 GB RAM and 750 GB hard disk. The operating system is 64 bits Microsoft Windows 10 and the computational platform is MATLAB R2018b. A medical skull image of size 444 × 535 × 3 uint8, in JPG format is used in this simulation as the original data which must be encrypted. The proposed scheme consists of two main parts: (a) chaotic key generation, (b) medical image encryption. The chaotic key generation phase takes 1.1057 seconds and encryption phase takes 0.7212 seconds. Thus, to generate the final encrypted images, the proposed scheme takes 1.8269 seconds which considering its high level of security, the speed of image encryption processing is acceptable. In addition, sometimes we don't need to encrypt all the data, especially where a faster speed is major requirement. For example, in a bank cheque/draft, only the seal of the bank, signature and amount need to be secure. Similarly, in the case of medical images we always only need to encrypt a specific portion of the image. In these cases for Decreasethe encryption time we can use the selective region based image encryption.

Remark 5. Motivations for considering chaotic encryption methods over traditional encryption schemes stem from the fact that these latter often exhibit, heightened security

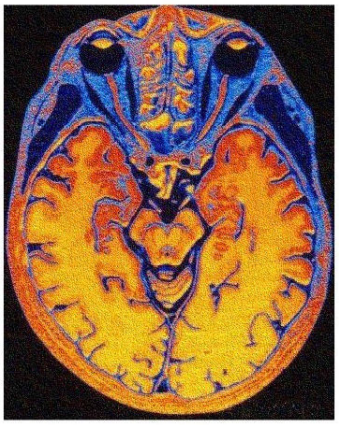

FIGURE 18. decrypted original image with some noise distortion and blurriness.

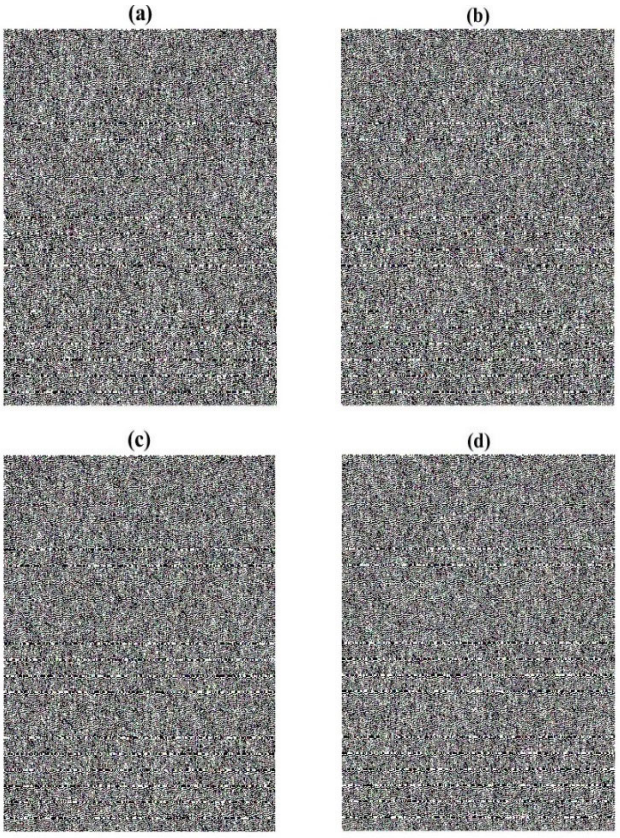

FIGURE 19. The encrypted images in the presence of 3% "salt & pepper" noise.

issues, high time consumption, key distribution problems and low-efficiency levels. Chaos-based encryptions are fast and advanced security algorithms exhibiting high sensitivity to the initial conditions, pseudo randomness property, and no periodicity and parameter dependency. These properties allow for supporting the permutation-diffusion requirement in cryptosystem establishment [53].

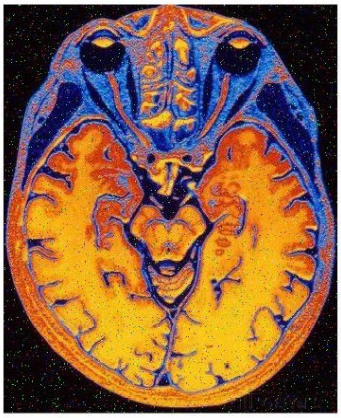

FIGURE 20. Decrypted original image with some noise distortion.

On the other hand, the symmetrical key cryptosystem (MORE Method) is a probabilistic symmetrical fully homomorphic Encryption method. Homomorphic Encryptions (HE) techniques such as the MORE method are new cryptographic research topics that were introduced to help users in preserving their data confidentiality and privacy by allowing untrusted parties to process computations over encrypted data. Althoughthere are many different image encryption algorithms such as fast image encryption algorithms, HE are highly sought after in real world modern applications such as Cloud Computing, Data aggregation in wireless sensor network scenario, Electronic Voting, Spam filters, etc. In such applications, HE will allow the creation of new techniques capable to run over encrypted inputs to produce encrypted outputs without knowing any information about the primitive data, once they are used by untrusted parties. Thus user's privacy is guaranteed [54]. However, traditional HE techniques exhibit some drawbacks including weakness against chosen/known plaintext attacks [54]. In this regard, one of the main advantages of the proposed method is the fact that it takes into consideration the above listed advantage of the MORE encryption method while at the same time eliminate some of its main disadvantages such as weakness against chosen/known plaintext attack using the chaotic encryption and different chaotic keys for encrypting each image pixel.

VII. CONCLUSION

This paper proposed a new fast reaching finite time synchronization approach for chaotic systems along with its application to medical image encryption. In this regard, an adaptive terminal sliding mode tracking controller with fast reaching condition was designed to synchronize the chaotic systems at the transmitter and receiver ends in finite time. The proposed approach was implemented to enhance the security of the medical image transmission and/or storage, by using the chaotic keys and combination of chaotic encryption method as chaotic MORE and XOR operation. The main objective of the suggested method was to remove all of the appearances of the original medical imageduring the transmission

or storage, while at the same time protecting the quality of the recovered medical image at an adequate level. The proposed approach was assessed using a simulation and analytical study. The obtained results showed that the suggested technique is robust, simple to implement and has a fast convergence rate. Additionally, the proposed cryptosystem was shown to yield an acceptable level of resistance to various attacks.

REFERENCES

[1] 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.
[2] 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.
[3] A. M. Anter and M. Ali, "Feature selection strategy based on hybrid crow search optimization algorithm integrated with chaos theory and fuzzy C-means algorithm for medical diagnosis problems," *Soft Comput.*, vol. 24, no. 3, pp. 1565–1584, Feb. 2020.
[4] 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.
[5] V. S. Afraimovich, N. N. Verichev, and M. I. Rabinovich, "Stochastic synchronization of oscillation in dissipative systems," *Radiophysics Quantum Electron.*, vol. 29, no. 9, pp. 795–803, Sep. 1986.
[6] E. Ott, C. Grebogi, and J. A. Yorke, "Controlling chaos," *Phys. Rev. Lett.*, vol. 64, no. 11, p. 1196, 1990.
[7] L. M. Pecora and T. L. Carroll, "Synchronization in chaotic systems," *Phys. Rev. Lett.*, vol. 64, no. 8, p. 821, 1990.
[8] 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.
[9] 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 (IS C)*, Jul. 2016, pp. 103–107.
[10] 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.
[11] 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.
[12] 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.
[13] X. Lu, "A financial chaotic system control method based on intermittent controller," *Math. Problems Eng.*, vol. 2020, pp. 1–12, Mar. 2020.
[14] 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.
[15] R. Wang, Y. Zhang, Y. Chen, X. Chen, and L. Xi, "Fuzzy neural network-based chaos synchronization for a class of fractional-order chaotic systems: An adaptive sliding mode control approach," *Nonlinear Dyn.*, vol. 100, no. 2, pp. 1275–1287, Apr. 2020, doi: 10.1007/s11071-020-05574-x.
[16] 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.
[17] J. Ni, L. Liu, C. Liu, and X. Hu, "Chattering-free time scale separation sliding mode control design with application to power system chaos suppression," *Math. Problems Eng.*, vol. 2016, pp. 1–14, Feb. 2016.
[18] J. Ni, L. Liu, C. Liu, and X. Hu, "Fractional order fixed-time nonsingular terminal sliding mode synchronization and control of fractional order chaotic systems," *Nonlinear Dyn.*, vol. 89, no. 3, pp. 2065–2083, Aug. 2017.
[19] Q. Lai, Z. Wan, A. Akgul, O. F. Boyraz, and M. Z. Yildiz, "Design and implementation of a new memristive chaotic system with application in touchless fingerprint encryption," *Chin. J. Phys.*, vol. 67, pp. 615–630, Oct. 2020.
[20] S. Hamidzadeh, A. Zarringhalam, and M. Yaghoobi, "Hyper chaos control using fuzzy sliding mode controller with application to a satellite motion," *Int. J. Comput. Appl.*, vol. 105, no. 4, pp. 1–5, Jan. 2014.
[21] P. Muthukumar, P. Balasubramaniam, and K. Ratnavelu, "Sliding mode control design for synchronization of fractional order chaotic systems and its application to a new cryptosystem," *Int. J. Dyn. Control*, vol. 5, no. 1, pp. 115–123, Mar. 2017.
[22] P. Jiang, B. Wang, H. Li, and H. Lu, "Modeling for chaotic time series based on linear and nonlinear framework: Application to wind speed forecasting," *Energy*, vol. 173, pp. 468–482, Apr. 2019.
[23] F. Shiravani and M. H. Shafiei, "Robust output regulation via sliding mode control and disturbance observer: Application in a forced Van Der Pol chaotic oscillator," *J. Dyn. Syst., Meas., Control*, vol. 139, no. 9, Sep. 2017, Art. no. 091015, doi: 10.1115/1.4036235.
[24] B. Wang, W. Li, X. Chen, and H. Chen, "Improved chicken swarm algorithms based on chaos theory and its application in wind power interval prediction," *Math. Problems Eng.*, vol. 2019, pp. 1–10, Jan. 2019.
[25] W. M. Bessa, A. S. de Paula, and M. A. Savi, "Chaos control using an adaptive fuzzy sliding mode controller with application to a nonlinear pendulum," *Chaos, Solitons Fractals*, vol. 42, no. 2, pp. 784–791, Oct. 2009.
[26] L. Chen, H. Yin, T. Huang, L. Yuan, S. Zheng, and L. Yin, "Chaos in fractional-order discrete neural networks with application to image encryption," *Neural Netw.*, vol. 125, pp. 174–184, May 2020.
[27] C.-C. Cheng, Y.-S. Lin, and S.-W. Wu, "Design of adaptive sliding mode tracking controllers for chaotic synchronization and application to secure communications," *J. Franklin Inst.*, vol. 349, no. 8, pp. 2626–2649, Oct. 2012.
[28] M. F. Hassan and M. Hammuda, "A new approach for constrained chaos synchronization with application to secure data communication," *J. Franklin Inst.*, vol. 356, no. 12, pp. 6697–6723, Aug. 2019.
[29] A. T. Azar and Q. Zhu, Eds., *Advances and Applications in Sliding Mode Control Systems* (Studies in Computational Intelligence), vol. 576. Cham, Switzerland: Springer, 2015.
[30] O. Boubaker and R. Dhifaoui, "Robust chaos synchronization for chua's circuits via active sliding mode control," in *Chaos, Complexity and Leadership*. Dordrecht, The Netherlands: Springer, 2012, pp. 141–151.
[31] J. Ni, L. Liu, C. Liu, X. Hu, and T. Shen, "Fixed-time dynamic surface high-order sliding mode control for chaotic oscillation in power system," *Nonlinear Dyn.*, vol. 86, no. 1, pp. 401–420, Oct. 2016.
[32] J. Zhang, X. Liu, Y. Xia, Z. Zuo, and Y. Wang, "Disturbance observer-based integral sliding-mode control for systems with mismatched disturbances," *IEEE Trans. Ind. Electron.*, vol. 63, no. 11, pp. 7040–7048, Nov. 2016.
[33] Y. Zhou and Z. Wang, "Robust motion control of a two-wheeled inverted pendulum with an input delay based on optimal integral sliding mode manifold," *Nonlinear Dyn.*, vol. 85, no. 3, pp. 2065–2074, Aug. 2016.
[34] Z.-L. Zhu, W. Zhang, K.-W. Wong, and H. Yu, "A chaos-based symmetric image encryption scheme using a bit-level permutation," *Inf. Sci.*, vol. 181, no. 6, pp. 1171–1186, Mar. 2011.
[35] Y. Wang, K.-W. Wong, X. Liao, and G. Chen, "A new chaos-based fast image encryption algorithm," *Appl. Soft Comput.*, vol. 11, no. 1, pp. 514–522, Jan. 2011.
[36] 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.
[37] 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.
[38] R. V. Nee and R. Prasad, *OFDM for Wireless Multimedia Communications*. Norwood, MA, USA: Artech House, 2000.
[39] S. Goldwasser and S. Micali, "Probabilistic encryption," *J. Comput. Syst. Sci.*, vol. 28, no. 2, pp. 270–299, Apr. 1984.
[40] A. Kipnis and E. Hibshoosh, "Efficient methods for practical fully homomorphic symmetric-key encrypton, randomization and verification," *IACR Cryptol. ePrint Arch.*, vol. 2012, p. 637, Nov. 2012.
[41] O. Mannai, R. Bechikh, H. Hermassi, R. Rhouma, and S. Belghith, "A new image encryption scheme based on a simple first-order time-delay system with appropriate nonlinearity," *Nonlinear Dyn.*, vol. 82, nos. 1–2, pp. 107–117, Oct. 2015.
[42] A. Levant, "On fixed and finite time stability in sliding mode control," in *Proc. 52nd IEEE Conf. Decis. Control*, Dec. 2013, pp. 4260–4265.
[43] Z. Sun, L. Si, Z. Shang, and J. Lei, "Finite-time synchronization of chaotic PMSM systems for secure communication and parameters identification," *Optik*, vol. 157, pp. 43–55, Mar. 2018.

[44] 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.
[45] M. Z. 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.
[46] C. Zhu and K. Sun, "Cryptanalyzing and improving a novel color image encryption algorithm using RT-enhanced chaotic tent maps," *IEEE Access*, vol. 6, pp. 18759–18770, 2018.
[47] 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.
[48] Z. Man, J. Li, X. Di, and O. Bai, "An image segmentation encryption algorithm based on hybrid chaotic system," *IEEE Access*, vol. 7, pp. 103047–103058, 2019.
[49] 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.
[50] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, vol. 28, no. 4, pp. 656–715, Oct. 1949.
[51] G. Chen, Y. Mao, and C. K. Chui, "A symmetric image encryption scheme based on 3D chaotic cat maps," *Chaos, Solitons Fractals*, vol. 21, no. 3, pp. 749–761, Jul. 2004.
[52] Y. Wu, J. P. Noonan, and S. Agaian, "NPCR and UACI randomness tests for image encryption," *Cyber J., Multidisciplinary J. Sci. Technol., J. Select. Areas Telecommu.*, vol. 1, no. 2, pp. 31–38, Apr. 2011.
[53] S. Hashemi, M. A. Pourmina, S. Mobayen, and M. R. Alagheband, "Design of a secure communication system between base transmitter station and mobile equipment based on finite-time chaos synchronisation," *Int. J. Syst. Sci.*, vol. 51, no. 11, pp. 1969–1986, Aug. 2020.
[54] K. Hariss, H. Noura, and A. E. Samhat, "Fully enhanced homomorphic encryption algorithm of MORE approach for real world applications," *J. Inf. Secur. Appl.*, vol. 34, pp. 233–242, Jun. 2017.

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

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 as 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.

SEYEDEH SOMAYEH HASHEMI was born in Zanjan, Iran, in 1982. She received the B.Sc. and M.Sc. degrees in electrical engineering from the Islamic Azad University (IAU), Naeen Branch, Esfahan, Iran, in 2004 and 2008, respectively, and the Ph.D. degree in communication engineering from the IAU, Science and Research Branch, Tehran, Iran, in 2020. Since 2009, she has been a full-time Member of the Department of Electrical Engineering, IAU, Abhar Branch. Since 2020, she has also 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.

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, and automotive engines.