IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 21 December 2023, accepted 6 February 2024, date of publication 9 February 2024, date of current version 23 February 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3364702

RESEARCH ARTICLE

Integrating RC6 Stream Cipher to a Chaotic Synchronization System

FENG-HSIAG HSIAO AND SHOU-WEN CHANG
Department of Electrical Engineering, National University of Tainan, Tainan 700301, Taiwan
Corresponding author: Feng-Hsiag Hsiao (fhhsiao@mail.nutn.edu.tw)

ABSTRACT With the advancement of technology, convenient communication fills every part of people's lives. However, the data may be stolen during the transmission process. Therefore, this study proposes a method based on the Takagi-Sugeno (T-S) fuzzy model using the Rivest Cipher 6 (RC6) algorithm in multiple time-delay chaotic systems. RC6 can be parameterized to support longer key lengths and encryption rounds, and RC6 has excellent computing speed and security. Nevertheless, quantum computers are getting universal. Studies have shown that existing encryption algorithms are unreliable in terms of security. Due to the mighty computing power of quantum computers, various encryption algorithms including RC6 will be cracked in a short period of time. Because chaos has the characteristics of disarray and irregularities, a systematic design combining chaotic synchronization with RC6 is presented to conduct double encryption to prevent attacks. In addition, we employ the improved genetic algorithm (IGA) to seek better fuzzy controller feedback gains than those sought by the genetic algorithm approach as well as the linear matrix inequality approach, and then to accelerate the synchronization. Subsequently, a synthesized fuzzy controller realizes exponential synchronization and achieves the optimal H^{∞} performance at the same time. Finally, the effectiveness of the proposed approach is demonstrated by an example with simulations.

INDEX TERMS Chaotic masking, Rivest cipher 6 algorithm, double encryption, exponential synchronization, optimal H^{∞} control, improved genetic algorithm.

I. INTRODUCTION

Convenient communication has permeated every aspect of people's lives as technology advances. However, with the continuous advancement of password-cracking technology, the security requirements of communication systems become more stringent. Therefore, the Rivest Cipher 6 (RC6) algorithm was used in this study to enhance security. The RC6 algorithm [1], [2], [3], [4], [5] is a symmetric-key algorithm derived from RC5. It was designed by Ron Rivest, Matt Robshaw, Ray Sidney, and Yiqun Lisa Yin to meet the Advanced Encryption Standard (AES) competition requirements. The RC6 algorithm was one of the five finalists [4]. Since its release, it has received attention and research from all parties [5], and has many technical applications. Longer key lengths and encryption rounds can be supported by parameterizing the RC6 algorithm. It has a block size of 128 bits and can support key sizes of 128, 192, and 256 bits up to 2040 bits. Many respects of RC6 and RC5 are similar [1], including structure, use of data-dependent rotations, modular addition, and XOR operations. RC6 employs an additional multiplication operation not found in the RC5 encryption algorithm. This operation causes every rotation to be determined by every bit in a word rather than the least significant few bits. RC6 is interweaving two parallel RC5 encryption processes, providing better encryption effect than RC5.

However, as computer computing power improves, quantum computers [6], [7], [8], [9] are expected to become more prevalent in the coming years. Traditional computers process data in bits, each switching between two states. Since two states can only be marked as 0 and 1, the data can only be processed in the most primitive order of 0 and 1. Nevertheless, the "quantum computer" exists 0 and 1 at the same time. This is known as "quantum superposition." Input and output data are regarded as mechanical quantities. All input and

The associate editor coordinating the review of this manuscript and approving it for publication was Chao-Yang Chen.

output can overlap, which is known as parallel processing; this advantage can improve the operation performance [7]. Quantum computers have much faster calculation speed than traditional computers. The quantum algorithm designed by Yang Liu and Shengyu Zhang in 2017 [6] can effectively improve the calculation speed and error rate compared with traditional algorithms. The fastest traditional computer currently takes billions of years to find all the prime factors of a 400-digit number, while a quantum computer may only take an hour or even a few minutes. Quantum algorithms outperform traditional algorithms in terms of calculation speed and accuracy while using the same computing and hardware resources [8]. When quantum computers become widely available, the existing symmetric and asymmetric encryption algorithms may be cracked in a very short period. However, the chaotic system is an excellent pseudo-random number generator that establishes foundations for subsequent encryption steps [10]. Chaos is characterized by disarray and irregularities. It is used to increase complexity, and then to enhance the security of cryptosystems. This research will introduce a double encryption technique which combines the RC6 algorithm and chaotic synchronization to reinforce prevention of security problems caused by quantum computers.

Chaotic encryption hides information in the chaotic masking signal's carrier wave. Due to the carrier waves' disarray and irregularities, a third party cannot determine the information the encryptor intends to transmit. In recent years, chaotic synchronization technology has provided new methods of communication security, such as chaotic encryption- and decryption-based communication systems, communication systems using chaos spreading codes for access among multiple users, and chaotic modulation-demodulation in digital and analog. Many encryption methods involved chaos theory. Chaotic maps have the properties of unpredictability and sensitivity to their parameters and initial values. They can generate different random sequences with different settings of parameters or initial values [11]. Meanwhile, chaotic synchronization technology and chaos security communication recently emerged as important research topics in communication at home and abroad [12], [13], [14], [15], [16], [17], [18], [19].

Pecora and Carroll first proposed the concept of chaotic synchronization in 1990 [12], [13]. Chaotic synchronization is the process of aligning the state trajectories of two chaotic systems. They were able to perform numerical simulations on Lorenz and Rössler systems successfully, and the results confirmed the feasibility of chaotic synchronization. Furthermore, the two further modified the chaotic circuit proposed by Newcomb and Sathyan [14], applied the concept of chaotic synchronization to the actual circuit. This aroused everyone's interest in determining how to achieve chaotic synchronization in communication security. In 1993, Cuomo et al. [15] completed Pecora and Carroll's synchronization method on the Lorenz circuit. They conducted two experiments on communication security. To complete the encrypted transmission of the signal, the terminal first uses the chaotic synchronization method to reproduce the masked signal and filter it from the received signal. Then, the terminal modifies the parameters to digitally process the synchronization result and obtain a binary signal. These two experiments established two of chaos' hot topics: chaotic synchronization and chaotic communication.

Different types of chaotic systems have different nonlinear terms, so the requirements for synchronous control may differ. The problem of synchronization is commonly associated when discussing chaotic communication. Many studies have been conducted on the academic synchronization control. In 2001, Lian et al. [16] successfully designed four fuzzy-based chaotic synchronization methods, and that can be applied to chaotic communication. In 2018, Ren et al. [11] proposed an encryption method based on computer-generated hologram and two-dimensional Sine Logistic modulation map, a kind of high-dimensional chaotic map. In the same year, Liu et al. [17] used three pseudo-random sequences, generated by three-dimensional chaos map, as the measurement matrix of compressed sensing and two random-phase masks in the asymmetric fractional wavelet transform. In 2022, Fradkov and Andrievsky [18] designed a discrete-time adaptive synchronization for signal transmission for time-varying nonlinear systems. In the same year, Mishra et al. [19] used Lyapunov's stability theory to design finite-time chaotic synchronization. The synchronization speed affects the transmission speed when using chaotic synchronization to transmit information. This issue should be considered during the design process to achieve synchronization quickly. Most research on chaotic synchronization assumes that the master and the slave systems are the same chaotic system. However, the structures and parameters of the master and slave chaotic systems are often not completely consistent in the real system application, affecting the synchronization results. Furthermore, time delays caused by the transmission of information are common in various engineering systems. Time-delay is an undesirable phenomenon in synchronization system, and an effective controller is expected to suppress it. Hence, related studies have widely investigated the problem of stability analysis in time-delay systems. Time delays have acquired increasing attention with respect to chaotic systems since Mackey and Glass [20] first demonstrated the chaotic phenomena in time delay systems. Time-delay can bring about inaccurate feedback control behaviours, and then result in the instability and non-synchronous phenomena of chaotic systems.

This study will use the improved genetic algorithm (IGA) to search for better fuzzy controller parameters. The genetic algorithm (GA) [21], [22], [23], [24], [25] was proposed by John Holland, a professor at the University of Michigan in 1975 [21]. Its basic concept is derived from Darwin's theory of natural selection, while the schema theorem is based on binary strings of specific digits being used as individuals of

artificial chromosomes to simulate gene evolution generation. Its primary goal is to frame the evolution of natural biological systems and stimulate significant breakthroughs in developing natural and artificial systems.

In 2014, Bailey et al. [23] confirmed the feasibility of using GA to generate graphical models for complex networks automatically. In 2011 [22], there was also research on the use of GA for synchronous optimization design. Recently, genetic algorithm has been widely used to search for the best solutions to various problems. The basic operators of biological species are used to evolve between generations. Therefore, GA is based on the biological concept of ''the winner of the inferior, the fittest.'' The concept of survival influenced the development of optimization techniques. GA follows a series of cyclic process similar to gene evolution, and its calculation steps include population generation, evaluation, and GA operation. In order to obtain a better fitness value, many improved genetic algorithms have been proposed [26], [27], [28], [29], [30], and the biggest difference between IGA [27], [28] used in this study and GA lies in the way of mating. GA randomly places the chromosomes after mating to obtain the best local solution [25], whereas IGA arranges the chromosomes after mating in the central and border areas to search for the global best solution [26]. Therefore, IGA is more likely than GA to generate excellent new individuals with a better fitness value. Many studies have been conducted to optimize the system using IGA [28], [29].

This study proposes a new fuzzy control method based on an IGA that employs the Parallel Distributed Compensation (PDC) technology to achieve the exponential synchronization of two chaotic systems with multiple time delays. In addition, combining the chaotic synchronization and cryptography concepts will result in a more secured communication system. To ensure the exponential stability of the error system, the initial message (plaintext) is first encrypted using the RC6 algorithm and the key, and the encrypted message (ciphertext) is re-encrypted through chaotic synchronization, and exponential stability related to time delay is derived by using the Lyapunov function criterion. Afterward, the exponential stability criterion is transformed into linear matrix inequality (LMI). A set of fuzzy controller parameters is obtained by using the LMI Toolbox of the numerical simulation software MATLAB. These parameters are evolved by the primitive populations of the IGA. Given IGA's ability to randomly search for the best solution in the entire domain, it is possible to find a better fuzzy controller feedback gain to accelerate the error system's convergence, allowing the master and slave systems to achieve synchronization quickly. In the past, feedback gains were resolved through trial-and-error and empirical methods. Therefore, there is a desire to develop better tools and methods to solve for suitable feedback gains. As such, this study constructed a new algorithm using IGA to solve the problem of feedback gains. The IGA approach seeks better feedback gains than those sought by the LMI approach, and speeds up the synchronization.

The remainder of this study is organized as follows. We establish the Takagi-Sugeno fuzzy models for representing chaotic systems, and some background about RC6 algorithm is given in section II. In section III, a robust fuzzy control scheme is proposed to accomplish the exponential optimal H^{∞} synchronization. The design algorithm is shown in section IV. In section V, the effectiveness of the proposed approach is demonstrated by an example with simulations. The findings and discussions for the proposed approach are presented in Section VI. Finally, the conclusions are drawn in section VII.

II. PROBLEM FORMULATION

This study utilized a master-slave configuration with two multiple time-delay chaotic (MTDC) systems. The dynamics of the master system (N_m) and the slave system (N_s) are as follows:

$$N_m : \dot{X}(t) = f(X(t)) + \sum_{k=1}^{g} H_k(X(t-\tau_k)) \tag{1}$$

$$N_s : \dot{\widehat{X}}(t) = \widehat{f}(\widehat{X}(t)) + \sum_{k=1}^{g} \widehat{H}_k(\widehat{X}(t-\tau_k)) + D(t) \tag{2}$$

where t is the variable of time, $\tau_k (k = 1, 2, \ldots, g)$ are the time delays, $f(\cdot), H_k(\cdot), \hat{f}(\cdot)$ and $\widehat{H}_k(\cdot)$ are the nonlinear vector-valued functions, $D(t)$ is the external interference, $\dot{X}$ is the state vector of the master system, and $\dot{\widehat{X}}$ is the state vector of the slave system.

A. RIVEST CIPHER 6

RC6 is a symmetric-key algorithm derived from RC5. Designed by Ron Rivest, Matt Robshaw, Ray Sidney, and Yiqun Lisa Yin in 1998, RC6 can be parameterized to support longer key lengths and encryption rounds. Figure 1 shows the RC6 encryption/decryption process.

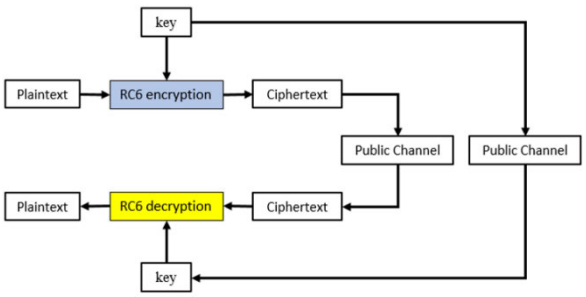

FIGURE 1. RC6 algorithm process.

Figure 2 illustrates the encryption procedure of RC6. The decryption process is to invert the structure by converting the addition operation into a subtraction operation.

This study chose to use RC6 due to its excellent calculation speed and security. Table 1 and Figure 3 illustrate the required execution time for RC6, Twofish, and Rijndael (AES) based on the 16-bytes key size for different file types and sizes. Meanwhile, Table 2 and Figure 4 show the required execution time for RC6, Twofish, and Rijndael (AES) based on the

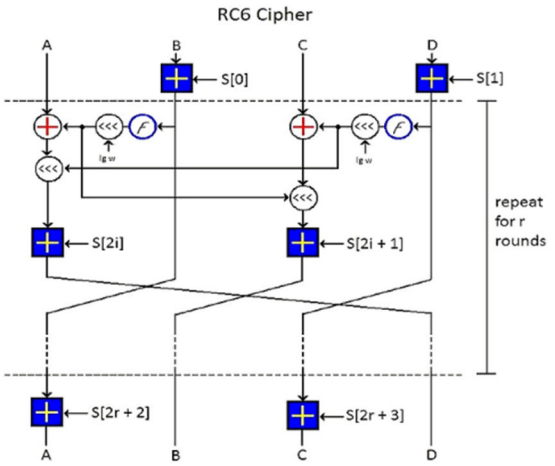

FIGURE 2. RC6 block cipher.

32-bytes key size for different file types and sizes. Figure 3 and Figure 4 depict RC6's excellent execution efficiency under different file types, sizes, and key lengths. The execution time of RC6 is shown in orange, Twofish in grey, and Rijndael (AES) in yellow. Finally, Table 3 summarizes the comparison of the different design parameters such as word size, block size, round number, and key size [02, 03].

TABLE 1. Comparison for 16-bytes key.

File Name (file type)	File Size (in KB)	RC6	Twofish	Rijndael (AES)
A.doc	712	200.8125	232.5	229.65
B.pdf	649	178.5	205	214.625
C.jpg	656	196.45	224.5	232.75
D.gif	1396	258.925	314.75	309.5
E.mp3	2068	320	383.5	380.45
F.avi	2800	357.5	426.735	435

TABLE 2. Comparison for 32-bytes key.

File Name (file type)	File Size (in KB)	RC6	Twofish	Rijndael (AES)
A.doc	712	209.75	256.95	268.125
B.pdf	649	187.5	213.75	228.75
C.jpg	656	209.8125	241.5	253.45
D.gif	1396	267.5125	329.75	333.85
E.mp3	2068	351.25	415.025	421.25
F.avi	2800	375	455.75	473.925

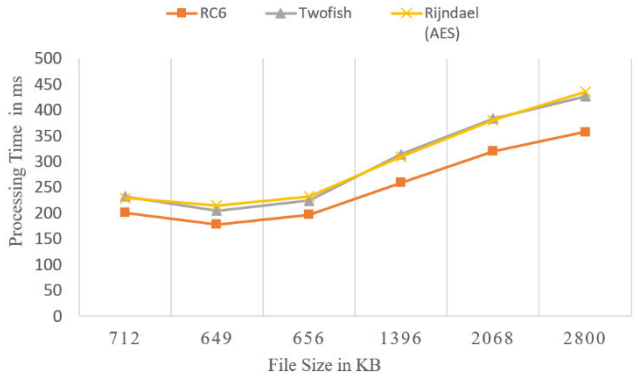

FIGURE 3. Processing time for 16-bytes key.

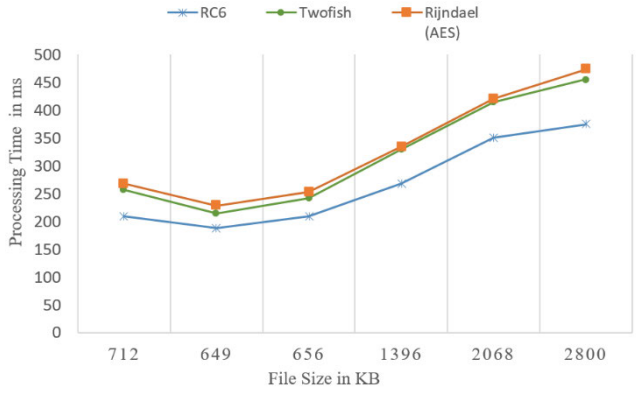

FIGURE 4. Processing time for 32-bytes key.

TABLE 3. Comparison on the basis of parameters.

Parameters	Algorithm Type		
	RC6	**Twofish**	**Rijndael**
b (key length in bytes)	0 - 255	16, 24 or 32	16, 24 or 32
r (number of rounds)	0 - 255 (standard 20)	16	10, 12, 14
Number of round keys	2r+4	2r+8	r+1
Block size in words	4w	4w	4w
w (word size in bits)	16, 32, 64 (standard 32)	16, 32, 64 (standard 32)	16, 32, 64 (standard 32)
Block size in bits	64, 128, 256 (standard 128)	64, 128, 256 (standard 128)	64, 128, 256 (standard 128)
Used Function	F(x) = x(2x+1) mod 2w	S-Box, MDS, PHT	SB, SR, MC, ARK, SB-1, SR-1, MC-1, S-Box

B. T-S (TAKAGI-SUGENO) FUZZY MODEL

Takagi and Sugeno [31] developed a fuzzy dynamic model three decades ago to represent locally linear input/output relationships of nonlinear systems. This dynamic model is characterized by IF-THEN rules; hence, it is used in this study to address the synchronization problem of MTDC systems.

The following is the ith rule of the T-S fuzzy model for the master system:

Rule i: IF $x_1(t)$ is M_{i1} and $\cdots$ and $x_\delta(t)$ is $M_{i\delta}$

$$\text{THEN } \dot{X}(t) = A_i X(t) + \sum_{k=1}^{g} \bar{A}_{ik} X(t-\tau_k)$$

where $i = 1, 2, \cdots, \phi$ and ϕ is the number of IF-THEN rules; A_i and $\bar{A}_{ik}$ are constant matrices with appropriate dimension; $M_{i\eta}(\eta = 1, 2, \cdots, \delta)$ are the fuzzy sets; $x_1(t) \sim x_\delta(t)$ are the premise variables. The final state of the fuzzy dynamic model is inferred as follows:

$$\begin{aligned}\dot{X}(t) &= \frac{\sum_{i=1}^{\phi} w_i(t)\left[A_i X(t) + \sum_{k=1}^{g} \bar{A}_{ik} X(t-\tau_k)\right]}{\sum_{i=1}^{\phi} w_i(t)} \\ &= \sum_{i=1}^{\phi} h_i(t)\left[A_i X(t) + \sum_{k=1}^{g} \bar{A}_{ik} X(t-\tau_k)\right] \quad (3)\end{aligned}$$

where $w_i(t) \equiv \prod_{\eta=1}^{\delta} M_{i\eta}\left(x_\eta(t)\right)$, and $M_{i\eta}\left(x_\eta(t)\right)$ denote the grade of membership of $x_\eta(t)$ in $M_{i\eta}$. Meanwhile, $h_i(t) \equiv \frac{w_i(t)}{\sum_{i=1}^{\phi} w_i(t)}$ and $\sum_{i=1}^{\phi} h_i(t) = 1$ for all t.

Similarly, the j th rule of the T-S fuzzy model for the slave system is proposed as follows:

Rule j : IF $\hat{x}_1(t)$ is $\widehat{M}_{j1}$ and $\cdots$ and $\hat{x}_\delta(t)$ is $\widehat{M}_{j\delta}$

$$\text{THEN } \hat{X}(t) = \hat{A}_j \hat{X}(t) + \sum_{k=1}^{g} \hat{\bar{A}}_{jk} \hat{X}(t-\tau_k) + D(t)$$

where $\hat{M}_{j\eta}(\eta = 1, 2, \cdots, \delta)$ are the fuzzy sets, $\hat{x}_1(t) \sim \hat{x}_\delta(t)$ are the premise variables, $\hat{A}_j$ and $\hat{\bar{A}}_{jk}$ are constant matrices with appropriate dimensions, and $j = 1, 2, \cdots, \sigma$ and σ is the number of IF-THEN rules. The final state of the fuzzy dynamic model is inferred as:

$$\begin{aligned}\hat{X}(t) &= \frac{\sum_{j=1}^{\sigma} \widehat{w}_j(t)\left[\hat{A}_j \hat{X}(t) + \sum_{k=1}^{g} \hat{\bar{A}}_{jk} \hat{X}(t-\tau_k) + D(t)\right]}{\sum_{j=1}^{\sigma} \widehat{w}_j(t)} \\ &= \sum_{j=1}^{\sigma} \hat{h}_j(t)\left[\hat{A}_j \hat{X}(t) + \sum_{k=1}^{g} \hat{\bar{A}}_{jk} \hat{X}(t-\tau_k)\right] + D(t) \\ &\quad (4)\end{aligned}$$

where $\widehat{w}_j(t) \equiv \prod_{\eta=1}^{\delta} \widehat{M}_{j\eta}\left(\hat{x}_\eta(t)\right)$, and $\widehat{M}_{j\eta}\left(\hat{x}_\eta(t)\right)$ denote the grade of membership of $\hat{x}_\eta(t)$ in $\hat{M}_{j\eta}$. Moreover, $\hat{h}_j(t) \equiv \frac{\widehat{w}_j(t)}{\sum_{j=1}^{\sigma} \widehat{w}_j(t)}$ and $\sum_{j=1}^{\sigma} \hat{h}_j(t) = 1$ for all t.

C. PARALLEL DISTRIBUTED COMPENSATION

The PDC scheme was used in this study to implement a control design based on a fuzzy model. Figure 5 shows that each control rule in the PDC scheme is designed for the corresponding rule of the T-S fuzzy model. Since a linear state equation describes each rule of the fuzzy model, the fuzzy controller is designed using the linear control theory. In general, the fuzzy blending of each individual linear controller achieves the overall nonlinear fuzzy controller. The fuzzy controller shares the same fuzzy sets as the fuzzy model in the premises [32].

The PDC scheme devises a model-based fuzzy controller to synchronize the slave system with the master system. The synchronization error is defined as

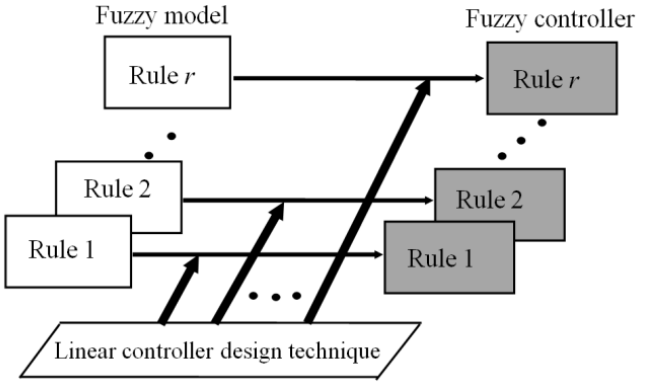

FIGURE 5. Parallel distributed compensation design.

$E(t) \equiv \hat{X}(t) - X(t) = [e_1(t), e_2(t), \cdots, e_\delta(t)]^T$, and the l th model-based fuzzy controller is depicted as follows:

The Control Rule l:

IF $e_1(t)$ is $\bar{M}_{l1}$ and $e_\delta(t)$ is $\bar{M}_{l\delta}$

$$\text{THEN } U(t) = -K_l E(t)$$

where $\bar{M}_{l\eta}(\eta = 1, 2, \cdots, \delta)$ are the fuzzy sets, K_l is the feedback gains, and $l = 1, 2, \cdots, \sigma$ and σ is the number of IFTHEN rule of the fuzzy controller. The final output of the fuzzy controller can be inferred as follows [33]:

$$U(t) = \frac{-\sum_{l=1}^{\sigma} \bar{w}_l(t) K_l E(t)}{\sum_{l=1}^{\sigma} \bar{w}_l(t)} = -\sum_{l=1}^{\sigma} \bar{h}_l(t) K_l E(t) \quad (5)$$

where $\bar{w}_l(t) \equiv \prod_{\eta=1}^{\delta} \bar{M}_{l\eta}\left(e_\eta(t)\right)$, and $\bar{M}_{l\eta}\left(e_\eta(t)\right)$ is the grade of membership of $e_\eta(t)$ in $M_{l\eta}$. Moreover, $\bar{h}_l(t) \equiv \frac{\bar{w}_l(t)}{\sum_{l=1}^{\sigma} \bar{w}_l(t)}$ and $\sum_{l=1}^{\sigma} \bar{h}_l(t) = 1$ for all t.

From the above, the T-S fuzzy models of the master and the slave chaotic systems are shown below:

Master:

$$\dot{X}(t) = \sum_{i=1}^{\phi} h_i(t)\left[A_i X(t) + \bar{A}_{ik} X(t-\tau_k)\right] + m \quad (6)$$

Slave:

$$\begin{aligned}\dot{\hat{X}}(t) = &\sum_{j=1}^{\sigma} \hat{h}_j(t)\left[\hat{A}_j \hat{X}(t) + \sum_{k=1}^{g} \hat{\bar{A}}_{jk} \hat{X}(t-\tau_k)\right] \\ &+ BU(t) + D(t) \quad (7)\end{aligned}$$

where m is the encrypted message and B is a real matrix. The controller gains $K_l(l = 1, 2, \cdots \sigma)$ are adjusted to synchronize the slave system (7) with the master system (6) as soon as possible.

D. IMPROVED GENETIC ALGORITHM

The GA approach seeks better feedback gains than the LMI approach to accelerate synchronization. Moreover, the IGA seeks better feedback gains than the GA approach and speeds up synchronization. To improve the performance of the GA-based control gain design, the IGA was used in this study, as verified and proposed by Leung et al. [26]. The key points of the IGA suggest that the chromosomes are averagely arranged in the central and boundary regions of the search domain after the crossover. The crossover gives

the next generation more potential to locate global optimal solutions. The improved crossover is stated as follows [26] and [27]:

$$os_c^1 = \left[\, os_1^1 \quad os_2^1 \quad \cdots \quad os_{no}^1 \,\right] = \frac{P_1 + P_2}{2} \tag{8}$$

$$\begin{aligned} os_c^2 &= \left[\, os_1^2 \quad os_2^2 \quad \cdots \quad os_{no}^2 \,\right] \\ &= P_{MAX}(1-w) + \mathrm{MAX}\,(P_1, P_2)\, w \end{aligned} \tag{9}$$

$$\begin{aligned} os_c^3 &= \left[\, os_1^3 \quad os_2^3 \quad \cdots \quad os_{no}^3 \,\right] \\ &= P_{min}(1-w) + \min\,(P_1, P_2)\, w \end{aligned} \tag{10}$$

$$\begin{aligned} os_c^4 &= \left[\, os_1^4 \quad os_2^4 \quad \cdots \quad os_{no}^4 \,\right] \\ &= \frac{(P_{MAX} + P_{min})\,(1-w) + (P_1 + P_2)\, w}{2} \end{aligned} \tag{11}$$

in which

$$P_{MAX} = \left[\, para_{MAX}^1 \; para_{MAX}^2 \cdots para_{MAX}^{no_{vars}} \,\right] \tag{12}$$

$$P_{min} = \left[\, para_{min}^1 \; para_{min}^2 \cdots para_{min}^{no_{vars}} \,\right] \tag{13}$$

where P_1 and P_2 are the two chromosomes selected from the parent, $os_c^1 \sim os_c^4$ are the chromosomes of the next generation, $\min\,(P_1, P_2)$ and $\max\,(P_1, P_2)$ are the new chromosomes where the genes are the minimum and maximum genes in P_1 and P_2, and $para_{min}^{\alpha}$, $para_{max}^{\alpha}$ are the lower and upper bounds of the α th genes in the search domain. The parameter w $\in [0, 1]$ is arbitrarily selected. Eqs. (9), (10) and Eqs. (8), (11) create two new chromosomes allotted in the boundary area and in the central area, respectively, of the search space.

In this study, the fitness function is defined as:

$$Fit(\Lambda) = \frac{1}{1 + \sum_{t=0}^{t} \sum_{\eta=0}^{\delta} \left| e_{\Lambda}^{\eta}(t) \right|} \tag{14}$$

where $Fit(\Lambda)$ is the fitness value of Λ th chromosome in the population. $e_{\wedge}^{\eta}(t)$ is the error of the Λ th chromosome in the population. η represents the number of chromosomes and Λ represents the generation of chromosomes. t_f denote the calculation length of the fitness function.

A mutation can change the genes of chromosomes, thereby modifying the inherited characteristics from parents [27]. The mutation process results in the generation of three new offspring, which are described as follows:

$$\begin{aligned} nos_j = &\left[\, os_1 \; os_2 \cdots os_{no_{vars}} \,\right] \\ &+ \left[\, b_1 \Delta os_1 \quad b_2 \Delta os_2 \quad \cdots \quad b_{no_{vars}} \Delta os_{no_{vars}} \,\right], \\ &j = 1, 2, 3 \end{aligned} \tag{15}$$

where b_i, $i = 1, 2, 3, \ldots, no_{vars}$ is a value of 0 or 1 and Δos_i, $i = 1, 2, 3, \ldots, no_{vars}$ are randomly generated numbers such as $para_{min}^{i} \le os_i + \Delta s_i \le para_{max}^{i}$. According to Eq. (15), The first one ($j = 1$) is obtained by allowing one b_i to be one, and the others are zeros. Meanwhile, based on Eq. (15), the second ($j = 2$) is obtained by having some of the b_i set to one. Eq. (15) shows that the third ($j = 3$) is obtained by setting all of the b_i to one. The fitness function given in Eq. (14) evaluates the validity of these three new offspring.

As shown in the given equation, a real number is randomly generated and compared with a user-defined number $f_f \in [0, 1]$. If the real number is smaller than f_f, the one with the highest fitness value among the three new offspring will replace the chromosome with the smallest fitness f_s in the population. If the real number is greater than f_f, the first posterity $\mathbf{nos}_1$ will replace the chromosome with the smallest fitness value f_s in the population, if $f\,(\mathbf{nos}_1) > f_s$; the second and third offspring will do the same. f_f successfully reduces the feasibility of convergence to a local optimum by accepting a bad posterity [27].

III. STABILITY ANALYSIS AND CHAOTIC SYNCHRONIZATION

This section inspects the synchronization of multiple timedelay chaotic (MTDC) systems using the modeling errors' influence. The exponential synchronization scheme for the MTDC systems is depicted as follows.

A. ERROR SYSTEM

According to Eqs. (1) and (2), we define the synchronization error as:

$$E(t) \equiv \hat{X}(t) - X(t) = [e_1(t), e_2(t), \cdots, e_{\delta}(t)]^T$$

The dynamics of the error system [34] with the fuzzy control can be depicted below:

$$\begin{aligned} \dot{E}(t) &= \widehat{\Psi} - \Psi + D(t) \\ &= \sum_{i=1}^{\phi} \sum_{l=1}^{\sigma} h_i(t)\bar{h}_l(t) \\ &\quad \times \left[G_{il} E(t) + \sum_{k=1}^{g} \bar{A}_{ik} E\,(t - \tau_k) \right] \\ &\quad + D(t) + \Phi(t) \end{aligned} \tag{16}$$

in which

$$\begin{aligned} G_{il} &\equiv A_i - BK_l \\ \widehat{\Psi} &\equiv \hat{f}(\hat{X}(t)) + \sum_{k=1}^{g} \widehat{H}_k \left(\hat{X}\,(t - \tau_k) \right) + U(t) \\ \Psi &\equiv f(X(t)) + \sum_{k=1}^{g} H_k\,(X\,(t - \tau_k)) \end{aligned}$$

with

$$\begin{aligned} U(t) &= -\sum_{l=1}^{\sigma} \bar{h}_l(t) K_l E(t) \\ \Phi(t) &\equiv \widehat{\Psi} - \Psi - \left\{ \sum_{i=1}^{\phi} \sum_{l=1}^{\sigma} h_i(t)\bar{h}_l(t) \left[G_{il} E(t) \right.\right. \\ &\quad \left.\left. + \sum_{k=1}^{g} \bar{A}_{ik} E\,(t - \tau_k) \right] \right\}. \end{aligned}$$

There is a $\Phi(t)$ between closed-loop nonlinear subsystem and the closed-loop fuzzy model, $\Phi(t)$ is the modeling error. Suppose that exists a bounding matrix $\varepsilon_{il}^{qq} R$ such that:

$$\|\Phi(t)\| \le \sum_{i=1}^{\Phi} \sum_{l=1}^{\sigma} h_i(t)\bar{h}_l(t)\varepsilon_{il}^{qq} RE(t) \tag{17}$$

in which $\left\|\varepsilon_{il}^{qq}\right\| \le 1$, for $i = 1, 2, \cdots, \phi$; $l = 1, 2, \cdots, \sigma$ and R denotes the specified structured bounding matrix. From Eq. (17), we have:

$$\begin{aligned} &\Phi^T(t)\Phi(t) \\ &\le \sum_{i=1}^{\Phi} \sum_{l=1}^{\sigma} h_i(t)\bar{h}_l(t) \left[\varepsilon_{il}^{qq} RE(t) \right]^T \end{aligned}$$

$$\sum_{i=1}^{\Phi}\sum_{l=1}^{\sigma} h_i(t)\bar{h}_l(t)\varepsilon_{il}^{qq}RE(t) \le [RE(t)]^T[RE(t)] \quad (18)$$

Specifically, $\Phi(t)$ is bounded by the specified structured bounding matrix R.

Remark 1 [35]: A small bounding matrix was first chosen to satisfy the stability conditions. The validity of Eq. (17) is then checked in the simulation. If Eq. (17) fails, the bounds for all elements in $\varepsilon_{il}^{qq}R$ can be expanded and the design procedure can be repeated until Eq. (17) holds.

$$\varepsilon_{il}^{qq}R = \begin{bmatrix} \varepsilon_{il}^{11} & 0 & 0 \\ 0 & \varepsilon_{il}^{22} & 0 \\ 0 & 0 & \varepsilon_{il}^{33} \end{bmatrix} \begin{bmatrix} r^{11} & r^{12} & r^{13} \\ r^{22} & r^{22} & r^{23} \\ r^{33} & r^{33} & r^{33} \end{bmatrix}$$

where $-1 \le \varepsilon_{il}^{qq} \le 1$ for $q = 1, 2, 3$. Notice that ε_{il}^{qq} can be chosen by other forms as long as $\left\|\varepsilon_{il}^{qq}\right\| \le 1$. The validity of Eq. (17) was then checked in the simulation. If it is not satisfied, the bounds for all elements in $\varepsilon_{il}^{qq}R_{il}$ can be expanded, and the design procedure can be repeated until Eq. (17) holds.

B. DELAY-DEPENDENT STABILITY CRITERION FOR EXPONENTIAL H^∞ SYNCHRONIZATION

This subsection proposes a delay-dependent stability criterion to ensure the exponential stability of the error system. Some lemma and definitions are provided below before inspecting the stability of the error system.

Lemma 1 [36]: For the real matrices A and B with appropriate dimension:

$$A^TB + B^TA \le aA^TA + a^{-1}B^TB$$

in which a is a positive constant.

Definition 1 [37], [38]: The slave system (2) can exponentially synchronize with the master system (1) if there exist two positive numbers α and β so that the synchronization error satisfies the following inequality:

$$\|E(t)\| \le \alpha \exp\left(-\beta\left(t - t_0\right)\right), \quad \forall t \ge t_0$$

in which the positive number β is referred to as the exponential convergence rate.

Definition 2 [39]: If the following conditions are satisfied, the master system (1) and slave system (2) are so called in exponential H^∞ synchronization:

(i). With zero disturbance (that is to say $D(t) = 0$), the error system with the fuzzy controller (5) is exponentially stable.

(ii). Setting the initial conditions to be zero (that is to say $E(t) = 0$ for $t \in [-\tau_{max}, 0]$, in which τ_{max} denotes the maximal value of τ_k) and a given constant $\rho > 0$, the following condition holds:

$$\Theta(E(t), D(t)) = \int_0^\infty E^T(t)E(t)dt - \rho^2\int_0^\infty D^T(t)D(t)dt \le 0 \quad (19)$$

in which the parameter ρ is the disturbance attenuation level. The parameter ρ is called the H^∞-norm bound of this controller. If the minimum ρ is found to meet the above conditions (that is to say the error system can exclude the exterior disturbance as strongly as possible), the fuzzy controller (5) is an optimal H^∞ synchronizer.

Theorem 1: For given the positive constants a, n, b, and ξ, if there exist two symmetric positive definite matrices ψ_k and P, so that the following inequalities hold, then the fuzzy controller (5) ensures the exponential H^∞ synchronization with the disturbance attenuation ρ:

$$\Delta_{il} \equiv \sum_{k=1}^{g} bG_{il}^TG_{il} + \sum_{k=1}^{g}\psi_k + ngR^TR + I + \sum_{k=1}^{g}\tau_k^2P^2\left(\xi^{-1} + n^{-1} + ga^{-1} + b^{-1}\right) < 0 \quad (20a)$$

$$\nabla_{ik} \equiv ga\bar{A}_{ik}^T\bar{A}_{ik} - \psi_k < 0 \quad (20b)$$

$$\rho > \sqrt{\xi g} \quad (20c)$$

where $G_{il} \equiv A_i - BK_l$, for $i = 1, 2, \cdots, \phi$; $l = 1, 2, \cdots, \sigma$ and $\tau_k (k = 1, 2, \cdots)$ are the time delays.

Proof: See the Appendix.

Corollary 1: Eq. (20a) and Eq. (20b) can be reformulated into LMIs using the following procedure:

The new variables are introduced: $Q = P^{-1}$, $G_{il} \equiv A_i - BK_l$ and $\overline{\psi_k} = Q\psi_kQ$. It is easy to demonstrate that the linear matrix inequalities in Eq. (20a) and Eq. (20b) are equivalent to the following LMIs in Eq. (21a) and Eq. (21b) based on Schur's complement [40]:

$$\begin{bmatrix} \Xi & QR^T & (A_i - BK_l)\,Q^T \\ RQ^T & -(ng)^{-1}I & 0 \\ Q\,(A_i - BK_l)^T & 0 & -(gb)^{-1}I \end{bmatrix} < 0 \quad (21a)$$

$$\begin{bmatrix} -\bar{\psi}_k & Q\bar{A}_{ik}^T \\ \bar{A}_{ik}Q & -(ga)^{-1}I \end{bmatrix} < 0 \quad (21b)$$

where

$$\Xi \equiv \sum_{k=1}^{g}\bar{\psi}_k + \sum_{k=1}^{g}\tau_k^2\left(\xi^{-1} + n^{-1} + ga^{-1} + b^{-1}\right)I + QIQ$$

Corollary 2: To accomplish exponential optimal H^∞ synchronization, the following constrained optimization problem formulates the fuzzy control design:

$$\text{minimize } \rho > \sqrt{\xi g} \quad (22)$$

subject to $\psi_k = \psi_k^T > 0, Q = Q^T$.

The positive constant ξ is minimized by the mincx function of MATLAB LMI Toolbox. Hence, we can get the minimum disturbance attenuation level $\rho_{min} > \sqrt{\xi_{min}g}$

Remark 2: In order to reduce the computational burden, this paper sets the positive constants a, n and b as unity.

Remark 3: According to Eq. (18), $\Phi(t)$ is assumed to be bounded by the specified structured bounding matrix R, and a larger $\Phi(t)$ results in a larger R. Since the matrices Δ_{il} must be a negative definite matric to meet the stability condition (20a), a larger R will make Eq. (20) more difficult to satisfy.

Remark 4: As inequality (20a) must be negative definite matric to meet the stability condition, a larger delay τ_k will make Theorem 1 more difficult to satisfy.

IV. ALGORITHM

In response to computers' increasing computing capacity, this study proposes a new encryption method that utilizes a doubleencryption technique. The proposed method combines the RC6 algorithm and chaotic synchronization to enhance information security. The block diagram (Figure 6) consists of an encrypter and a decrypter. T-S fuzzy models for the master and slave systems of two different multiple time-delay chaotic (MTDC) systems were developed. Using Lyapunov functions, an exponential stability criterion was obtained, and a fuzzy controller was designed based on this criterion to achieve rapid synchronization, and then improve the system's transmission rate.

The plaintext and the key were used to obtain the ciphertext through the encryption function of the RC6 algorithm (as shown in Figure 6, bottom left corner). The ciphertext is then forwarded to the master system. The ciphertext was further loaded into the carrier wave, which was constructed by the chaotic masking signal for the double encryption, using the characteristics of disarray and irregularities. In addition, this study employed the improved genetic algorithm (IGA) to accelerate the convergence of the error system during master-slave system synchronization, and to seek better fuzzy controller feedback gains to speed up the synchronization (Figure 6, middle section). When the slave system is synchronized with the master system, the encrypted signal is then sent to the slave system through the public channel (Figure 6, bottom right corner). Then, the slave system filtered the encrypted signal to obtain the ciphertext. Finally, the RC6 decryption algorithm decrypts the ciphertext using the key.

Step01. The plaintext and key are encrypted for the first time using the RC6 encryption algorithm to obtain the ciphertext.
Step02. The ciphertext is sent to the master system to add the chaotic masking signal to obtain the encrypted signal.
Step03. Takagi-Sugeno (T-S) fuzzy models of the master system (1) and the slave system (2) are established.
Step04. The synchronization error is defined by the state of the master system and the slave system, and the error system (16) is established.
Step05. Use the Lyapunov function to find an exponential stability.
Step06. A PDC fuzzy controller that can quickly achieve synchronization is designed according to the abovementioned exponential stability criterion.
Step07. Considering that the system will be disturbed by noise, the fuzzy controller is improved to optimal H^{∞} fuzzy controller to overcome the influence of noise on chaos synchronization.

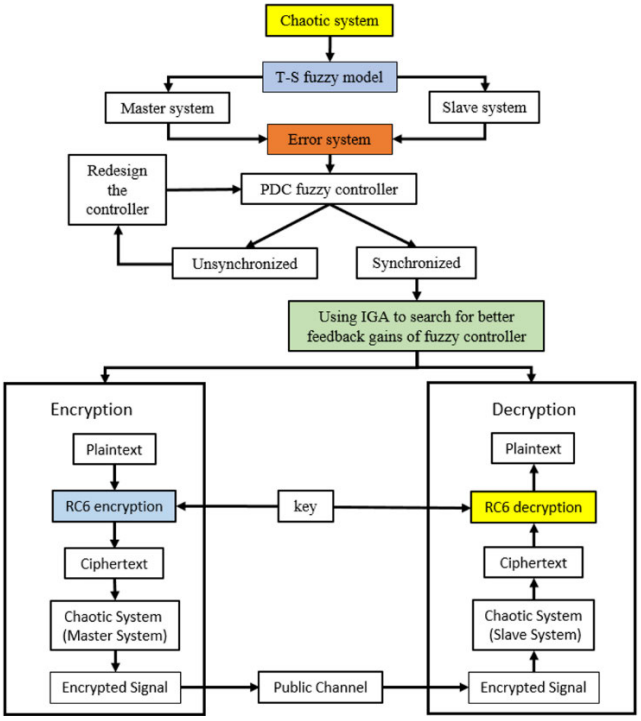

FIGURE 6. The chaotic synchronization cryptosystem.

Step08. Transforms the exponential stability criterion for the error system into an LMI form.
Step09. The parameters of the fuzzy controller satisfying the above LMI are obtained by using the LMI Toolbox of the numerical simulation software (MATLAB).
Step10. Evolving this parameter as the original population of the Improved Genetic Algorithm (IGA) to search for better fuzzy controller feedback gains to speed up the synchronization of the master and slave systems.
Step11. After the encrypted signal is transmitted through the public channel to filter the chaotic masking signal from the system, the ciphertext can be obtained.
Step12. Based on RC6 decryption function, the plaintext recovers from the ciphertext.

V. NUMERICAL EXAMPLE

The following example demonstrates the algorithm described in this study.

Problem: This example employed a fuzzy controller to achieve a secure, chaotic communication system. Consider the following modified multiple time-delay Genesio and Rossler chaotic systems in the master-slave configuration:

$$\begin{cases} \dot{x}_1(t) = 0.3 * [x_2(t) - x_1(t)] \\ \dot{x}_2(t) = -8.5 * x_1(t) - 0.2 * x_1(t) * x_3(t) \\ \dot{x}_3(t) = -5x_3(t) + 5x_1^2(t) + 0.3\, x_1(t - 0.05) \\ \qquad +0.3\, x_2(t - 0.1) + 0.3\, x_3(t - 0.09) \end{cases} \tag{23}$$

and

$$\begin{cases} \dot{\widehat{x_1}}(t) = -\widehat{x_2}(t) - \widehat{x_3}(t) + D_1(t) \\ \dot{\widehat{x_2}}(t) = \widehat{x_1}(t) + 0.2\widehat{x_2}(t) + D_2(t) \\ \dot{\widehat{x_3}}(t) = 0.43 + \widehat{x_1}(t)\widehat{x_3}(t) - 4.5\widehat{x_3}(t) \\ \qquad +\widehat{x_1}(t-0.06) + \widehat{x_2}(t-0.13) \\ \qquad +\widehat{x_3}(t-0.02) + D_3(t) \end{cases} \tag{24}$$

where $[x_1(t)x_2(t)x_3(t)]^T$ and $[\widehat{x_1}(t)\widehat{x_2}(t)\widehat{x_3}(t)]^T$ are the state vectors of the master and slave systems, respectively. Let the initial conditions of the master and slave systems be: $[x_1(0) = -0.2 \quad x_2(0) = -3 \quad x_3(0) = 0.4]$ and $[\widehat{x_1}(0) = -0.6\widehat{x_2}(0) = -0.4\widehat{x_3}(0) = 2]$, respectively, and let the external disturbance be:

$$\begin{aligned} D_1 &= 0.2 \times sin(1.3 \times t) \\ D_2 &= 0.1 \times cos(1.4 \times t) \\ D_3 &= 0.3 \times sin(0.5 \times t) \end{aligned} \tag{25}$$

Figure 7 and Figure 8 show the chaotic behaviors of the master (23) and slave (24) systems.

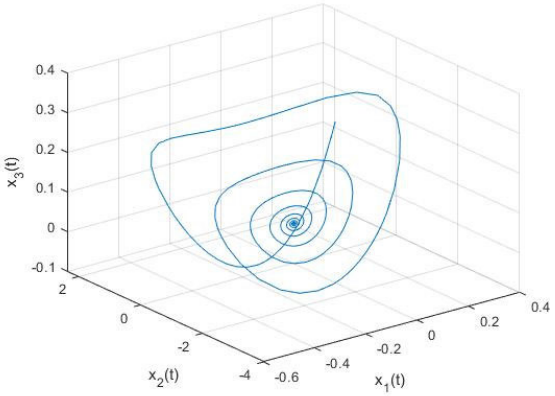

FIGURE 7. Chaotic behavior of the Genesio_master system (23).

Step1: Use RC6 encryption function to encrypt plaintext and key into ciphertext.

In this paper, the plaintext is "NUTNEE".

Set key as "M11082015".

Then, RC6 algorithm can be started in ECB mode to encrypt the plaintext.

The encrypted message is obtained:

"2b58839dc013b66e5c6c1d1808ad7a6b"

In order to combine the master system, the encrypted message is converted into decimal as

$$\begin{aligned} &57616395436226993457273318016337934955 \\ &(2B58839DC013B66E5C6C1D1808AD7A6B)_{16} \\ &= \left(2 \times 16^{31}\right) + \left(11 \times 16^{30}\right) + \left(5 \times 16^{29}\right) + \left(8 \times 16^{28}\right) \\ &\quad + \left(8 \times 16^{27}\right) + \left(3 \times 16^{26}\right) + \left(9 \times 16^{25}\right) \\ &\quad + \left(13 \times 16^{24}\right) + \left(12 \times 16^{23}\right) + \left(0 \times 16^{22}\right) \\ &\quad + \left(1 \times 16^{21}\right) + \left(3 \times 16^{20}\right) + \left(11 \times 16^{19}\right) \end{aligned}$$

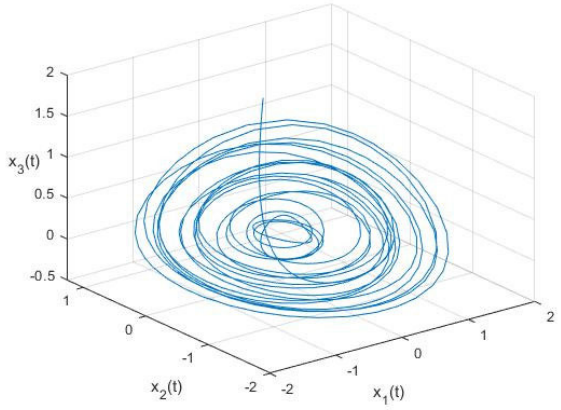

FIGURE 8. Chaotic behavior of the Rossler_slave system (24).

$$\begin{aligned} &+ \left(6 \times 16^{18}\right) + \left(6 \times 16^{17}\right) + \left(14 \times 16^{16}\right) \\ &+ \left(5 \times 16^{15}\right) + \left(12 \times 16^{14}\right) + \left(6 \times 16^{13}\right) \\ &+ \left(12 \times 16^{12}\right) + \left(1 \times 16^{11}\right) + \left(13 \times 16^{10}\right) \\ &+ \left(1 \times 16^{9}\right) + \left(8 \times 16^{5}\right) + \left(0 \times 16^{7}\right) + \left(8 \times 16^{6}\right) \\ &+ \left(10 \times 16^{5}\right) + \left(13 \times 16^{4}\right) + \left(7 \times 16^{3}\right) + \left(10 \times 16^{2}\right) \\ &+ \left(6 \times 16^{1}\right) + \left(11 \times 16^{9}\right) \\ &= (57616395436226993457273318016337934955)_{10} \end{aligned}$$

Because the value is huge, it is multiplied by 10^{-38}, and the encrypted message

$$0.57616395436226993457273318016337934955$$

Step2: The encrypted message m combines with the master system (23).

$$\begin{cases} \dot{x}_1(t) = 0.3 * [x_2(t) - x_1(t)] + m \\ \dot{x}_2(t) = -8.5 * x_1(t) - 0.2 * x_1(t) * x_3(t) \\ \dot{x}_3(t) = -5x_3(t) + 5x_1^2(t) + 0.3\, x_1(t-0.05) \\ \qquad +0.3\, x_2(t-0.1) + 0.3\, x_3(t-0.09) \end{cases} \tag{26}$$

Figure 9 shows the chaotic behaviors of the Genesio master (26) system with the encrypted message m.

Step3: A T-S fuzzy model is constructed for the system. In order to reduce as few rules as possible, the chaotic system (24,26) is expressed as the following fuzzy model:

The fuzzy model of the master system :

Rule 1 :

IF $\quad x_1(t)$ is M_{11},

Then $\quad \dot{X}(t) = A_1X(t) + \sum_{k=1}^{3} \bar{A}_{1k}X(t-\tau_k) + m \quad$ (27a)

Rule 2 :

IF $\quad x_1(t)$ is M_{21},

Then $\quad \dot{X}(t) = A_2X(t) + \sum_{k=1}^{3} \bar{A}_{2k}X(t-\tau_k) + m \quad$ (27b)

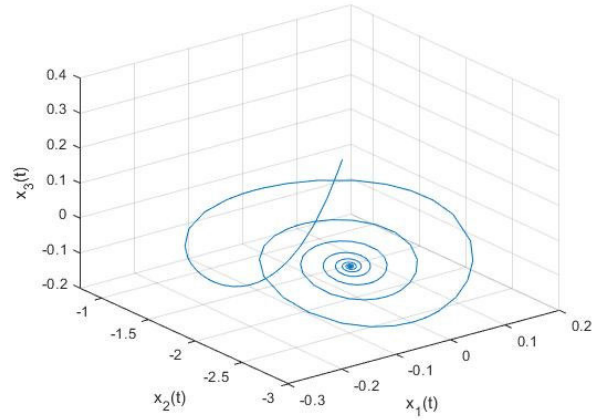

FIGURE 9. Chaotic behavior of the Genesio master system with m (26).

where $[x_1(t) \quad x_2(t) \quad x_3(t)]^T$,

$$\tau_1 = 0.05, \quad \tau_2 = 0.1, \quad \tau_3 = 0.09,$$

$$A_1 = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ -15.3110 & -3.5 & -2 \end{bmatrix},$$

$$A_2 = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ -15.7547 & -3.5 & -2 \end{bmatrix},$$

$$\overline{A_{11}} = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0.5 & 0 & 0 \end{bmatrix}, \overline{A_{21}} = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0.5 & 0 & 0 \end{bmatrix},$$

$$\overline{A_{12}} = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0.5 & 0 \end{bmatrix}, \overline{A_{22}} = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0.5 & 0 \end{bmatrix},$$

$$\overline{A_{13}} = \begin{bmatrix} 0 & 0 & 0.5 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}, \overline{A_{23}} = \begin{bmatrix} 0 & 0 & 0.5 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} \tag{28}$$

and the membership functions for Rules 1 and 2 are:

$$M_{11}(x_1(t)) = \begin{cases} 1 & x_1(t) \geq -15.311 \\ \dfrac{x_1(t) + 15.7547}{-15.311 + 15.7547} & -15.311 > x_1(t) > -15.7547 \\ 0 & x_1(t) \leq -15.7547 \end{cases}$$

$$M_{21}(x_1(t)) = 1 - M_{11}(x_1(t)) \tag{29}$$

The fuzzy model of the slave system :

Rule 1:

IF $\mathrm{x_1(t)}$ is $\mathrm{M_{11}}$,

Then $\dot{\hat{x}}(t) = \widehat{A_1}\hat{X}(t) + \sum_{k=1}^{3} \widehat{A_{1k}}\hat{X}(t - \tau_k) + D(t)$ (30a)

Rule 2:

IF $\mathrm{x_1(t)}$ is $\mathrm{M_{21}}$,

Then $\dot{\hat{x}}(t) = \widehat{A_1}\hat{X}(t) + \sum_{k=1}^{3} \widehat{A_{1k}}\hat{X}(t - \tau_k) + D(t)$ (30b)

where $[\widehat{x_1}(t)\widehat{x_2}(t)\widehat{x_3}(t)]^T$,

$$\tau_1 = 0.06, \quad \tau_2 = 0.13, \quad \tau_3 = 0.02$$

$$\widehat{A_1} = \begin{bmatrix} 0 & -1 & -1 \\ 1 & 0.2 & 0 \\ 0 & 0 & -2.6012 \end{bmatrix}, \widehat{A_2} = \begin{bmatrix} 0 & -1 & -1 \\ 1 & 0.2 & 0 \\ 0 & 0 & -6.6913 \end{bmatrix}$$

$$\widehat{\overline{A_{11}}} = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{bmatrix}, \widehat{\overline{A_{21}}} = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{bmatrix}, \widehat{\overline{A_{12}}} = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix},$$

$$\widehat{\overline{A_{22}}} = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}, \widehat{\overline{A_{13}}} = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \widehat{\overline{A_{23}}} = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix},$$

$$B = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \tag{31}$$

and the membership functions for Rules 1 and 2 are:

$$\widehat{M_{11}}(\widehat{x_1}(t)) = \begin{cases} 1 & \widehat{x_1}(t) \geq -2.6012 \\ \dfrac{\widehat{x_1}(t) + 6.6913}{-2.6012 + 6.6913} & -2.6012 > \widehat{x_1}(t) > -6.6913 \\ 0 & \widehat{x_1}(t) \leq -6.6913 \end{cases}$$

$$\widehat{M_{21}}(\widehat{x_1}(t)) = 1 - \widehat{M_{11}}(\widehat{x_1}(t)) \tag{32}$$

Step 4: To synchronize the slave system with the master system, a fuzzy controller is synthesized as below:

Control Rule 1:

IF $e_1(t)$ *is* M_1,

THEN $U(t) = -K_1E(t)$

Control Rule 2:

IF $e_1(t)$ is M_2,

THEN $U(t) = -K_2E(t)$ (33)

in which M_1 and M_2 denote the membership functions for each e_1 (see Figure 10):

$$M_1(e_1(t)) = \begin{cases} 1, & e_1(t) \geq 10 \\ (\dfrac{1}{(\frac{e_1(t)-3}{2})^4}), & e_1(t) \leq -10 \\ 0, & e_1(t) > -10 \end{cases}$$

$$M_2(e_1(t)) = \begin{cases} 0, & e_1(t) > -10 \\ (1 - \dfrac{1}{(\frac{e_1(t)-3}{2})^4}), & 10 > e_1(t) \leq -10 \\ 1, & e_1(t) > -10 \end{cases} \tag{34}$$

Based on Eq. (5), the fuzzy controller is obtained as:

$$U(t) = \frac{\sum_{l=1}^{2} w_l(t)K_lE(t)}{\sum_{l=1}^{2} w_l(t)} = -\sum_{l=1}^{2} \bar{h}_l(t)K_lE(t) \tag{35}$$

with $w_l(t) = M_1(e_1(t))$, $\bar{h}_l(t) \equiv \frac{w_l(t)}{\sum_{l=1}^{2} w_l(t)}$.

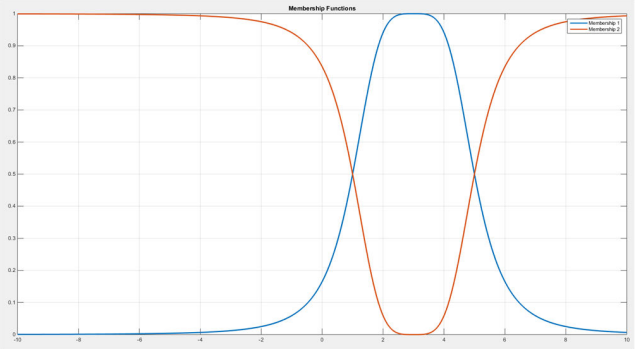

FIGURE 10. Membership of the controller.

According to Eq. (16), the dynamics of the error system is obtained as follows:

$$\dot{E}(t) = \sum_{i=1}^{2}\sum_{l=1}^{2} h_i(t)\bar{h}_l(t) \times \left[G_{il}E(t) + \sum_{k=1}^{3}\bar{A}_{ik}E\left(t-\tau_k\right)\right] + D(t) + \Phi(t) \tag{36}$$

where

$$G_{il} \equiv A_i - BK_l,$$
$$\hat{\Psi} \equiv \hat{f}(\hat{X}(t)) + \sum_{k=1}^{3}\widehat{H}_k\left(\hat{X}\left(t-\tau_k\right)\right) + U(t),$$

with

$$U(t) = -\sum_{l=1}^{2}\bar{h}_l(t)K_lE(t)$$
$$\Psi \equiv f(X(t)) + \sum_{k=1}^{3}H_k\left(X\left(t-\tau_k\right)\right)$$
$$\Phi(t) \equiv \hat{\Psi} - \Psi - \left\{\sum_{i=1}^{2}\sum_{l=1}^{2}h_i(t)\bar{h}_l(t)\left[G_{il}E(t) + \sum_{k=1}^{3}\bar{A}_{ik}E\left(t-\tau_k\right)\right]\right\}.$$

Step 5: In this article, we use IGA to aid in the design of feedback gains.

LMI

On the basis of Eqs. (27)-(36), the LMIs in Eqs. (21a) and (21b) can be solved by the MATLAB LMI Toolbox with $a = 1, n = 1, b = 1$, and the resulting feedback gains are:

$$K_1 = \begin{bmatrix} 416.0950 & 0.0002 & -0.0029 \\ 0.0002 & 416.0950 & -0.0005 \\ -0.0029 & -0.0005 & 416.0942 \end{bmatrix} \tag{37a}$$

$$K_2 = \begin{bmatrix} 416.0948 & 0.0002 & -0.0029 \\ 0.0002 & 416.0948 & -0.0005 \\ -0.0029 & -0.0005 & 416.0940 \end{bmatrix} \tag{37b}$$

IGA(LMI)

IGA has a random search ability for near-optimal solutions. Due to its search ability, IGA can seek better fuzzy controller feedback gains, thus, speeding up the synchronization. In addition, an increased distortion appears in the filter when the feedback gain becomes too large. The lower and upper bounds were set in this study. According to Eqs. (37a)-(37b), the feedback gains of the search space is set as $(L_{1x}, L_{2x}) \in [10^2, 10^4]$ and $(L_{1y}, L_{2y}) \in [-1, 1]$ for $x = 1, 5, 9; y = 2, 3, 4, 6, 7, 8$. Table 4 shows that the repeated experiments determine the values of w and P_m with the best fitness values.

TABLE 4. Comparison for 32-bytes key.

Population size	32
Number of generations	100
Method of reproduction	roulette wheel selection
Method of crossover	improved crossover Eqs. (8-11) with $w = 0.6$
Probability of mutation (P_m)	0.07
Coding of chromosome	real-numbered string
Fitness function	Eq. (14) with $t_f = 600$

For the IGA has the properties of search globalization and convergence speed. We tried a variety of w and P_m to provide IGA with better search efficiency. Table 5 shows that the fitness values of IGA involve 100 generations with fixed w and P_m.

After executing the IGA search process, the resulting feedback gains are obtained:

$$K_1 = 10^3 \times \begin{bmatrix} 7.2378 & 2.9923 & 2.6014 \\ 3.8361 & 7.7143 & 3.3107 \\ 3.8155 & 3.2546 & 8.5128 \end{bmatrix}$$

$$K_2 = 10^3 \times \begin{bmatrix} 8.6288 & 3.8936 & 4.5306 \\ 3.2325 & 7.8468 & 2.0663 \\ 3.3548 & 3.6364 & 7.1467 \end{bmatrix}$$

Evolutions of the fitness values are shown in Figure 11. The best parameters for IGA are shown in Figure 11 and Table 5.2. The fitness value is 0.77440984.

Step 6: According to Eqs. (27)-(37), the LMIs in Eq. (21a) and (21b) can be solved using the MATLAB LMI Toolbox. Following Remark 3.1, the specified structured bounding matrices R and ε_{il} are set as $R = \begin{bmatrix} 5000 & 0 & 0 \\ 0 & 5000 & 0 \\ 0 & 0 & 5000 \end{bmatrix}$, $\varepsilon_{il} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$. The positive constant ξ is minimized by the *mincx* function of the MATLAB LMI Toolbox: $\xi_{min} = 4.2683 * 10^{-7}$; the minimum disturbance attenuation level $\rho_{min} = 1.1 * 10^{-3}$ is thus obtained.

Step 7: The common solutions $Q, F_1, F_2, \psi_1, \psi_2$ and ψ_3 of the stability conditions (20a) and (20b) can be obtained with

TABLE 5. The fitness values of IGA with various w and P_m.

w \ Pm	0.01	0.02	0.03	0.04	0.05
0.1	0.72440	0.69983	0.70867	0.68712	0.68686
0.2	0.75347	0.67313	0.68223	0.75184	0.72395
0.3	0.69817	0.71703	0.71859	0.71038	0.70572
0.4	0.69844	0.72478	0.77406	0.68677	0.76803
0.5	0.72042	0.77087	0.69970	0.76833	0.73933
0.6	0.67222	0.68229	0.69748	0.75741	0.71899
0.7	0.67128	0.69185	0.76201	0.70098	0.68334
0.8	0.71072	0.70603	0.75070	0.71752	0.76958
0.9	0.74480	0.69911	0.67102	0.70451	0.71509

(1)

w \ Pm	0.06	0.07	0.08	0.09	0.1
0.1	0.77107	0.67731	0.76243	0.74635	0.75803
0.2	0.70311	0.76158	0.73629	0.68339	0.74130
0.3	0.71284	0.69178	0.67032	0.71100	0.67869
0.4	0.69556	0.73068	0.74618	0.70602	0.76845
0.5	0.72609	0.67242	0.69148	0.69270	0.72048
0.6	0.77245	0.77440	0.76483	0.73091	0.73721
0.7	0.69111	0.75268	0.71863	0.76771	0.75524
0.8	0.71854	0.73510	0.74243	0.74315	0.72271
0.9	0.70606	0.67865	0.73372	0.74209	0.69154

(2)

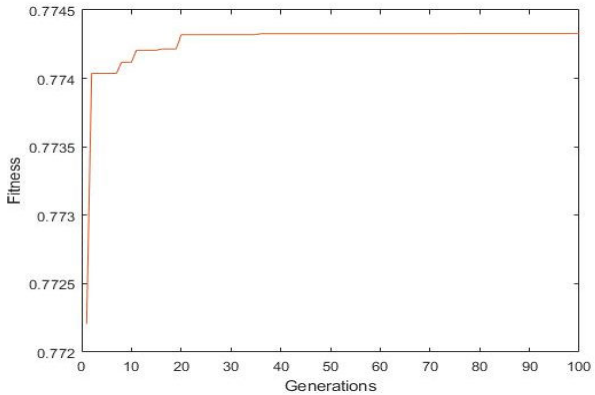

FIGURE 11. Fitness values of IGA.

the best value t_{min} of LMI Solver (MATLAB), which is $-1.0371 * 10^4$:

$$Q = 10^{-3} \times \begin{bmatrix} 0.2658 & -0.0839 & -0.0847 \\ -0.839 & 0.2599 & -0.0575 \\ -0.0847 & -0.0575 & 0.2572 \end{bmatrix}$$

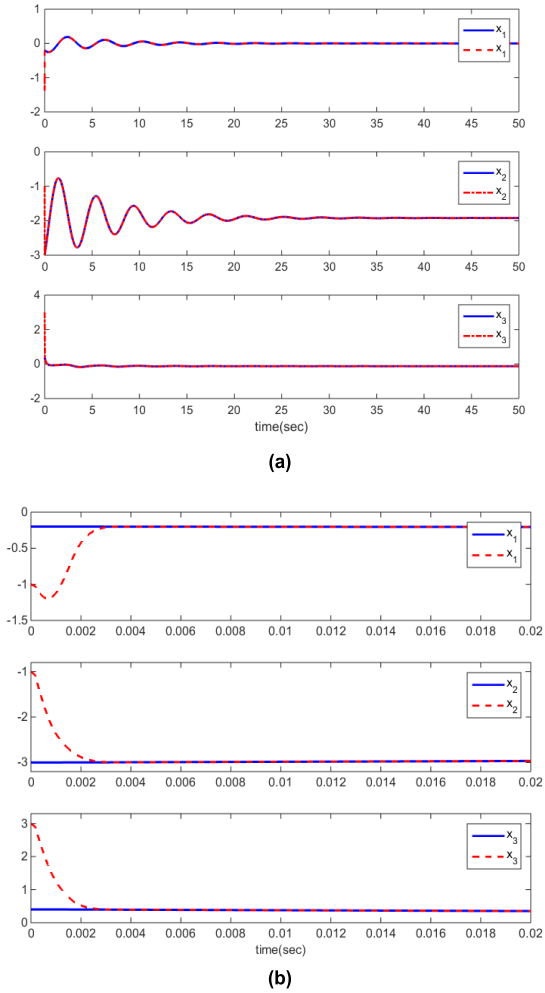

FIGURE 12. (a) State responses of both master and slave systems (t = 0 50 sec). (b) State responses of both master and slave systems (t = 0 0.02 sec).

$$P = Q^{-1} = 10^3 \times \begin{bmatrix} 5.1255 & 2.1342 & 2.1650 \\ 2.1342 & 4.9368 & 1.8060 \\ 2.1650 & 1.8060 & 5.0048 \end{bmatrix}$$

$$\bar{\psi}_1 = \bar{\psi}_2 = \bar{\psi}_3 = \begin{bmatrix} 19.4646 & 1.8834 & 0.7212 \\ 1.8834 & 20.4253 & 1.4763 \\ 0.7212 & 1.4763 & 21.6891 \end{bmatrix}$$

Figure 12 displays the state responses of both master and slave systems. The chaotic behaviors of the master and slave systems are shown in Figure 13. Furthermore, the assumption of Eq. (17) is satisfied shown in Figure 14.

$$\|\Phi(t)\| \leq \sum_{i=1}^{\Phi} \sum_{l=1}^{\sigma} h_i(t)\bar{h}_l(t)\varepsilon_{il}^{qq} RE(t) \qquad \text{(see(17))}$$

Step 8: When the slave system synchronizes with the master system, the plaintext can be restored from the output error signal and the decryption function. The encrypted message m is thus obtained:

0.576163954362269934572733180163379349 55

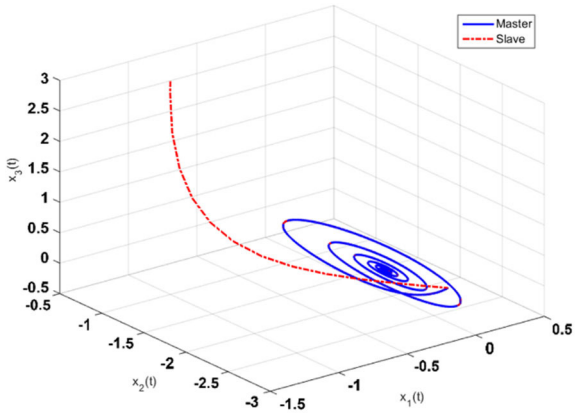

FIGURE 13. The chaotic behaviors of the master and slave systems.

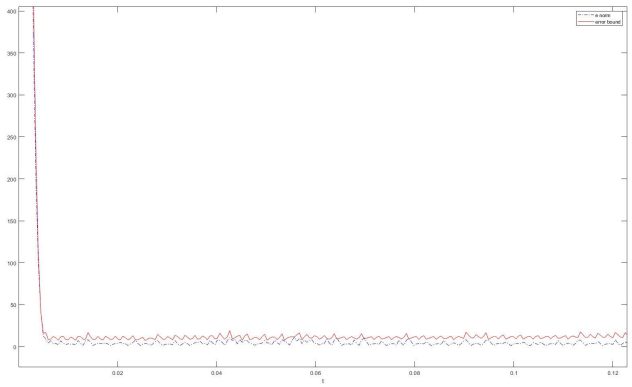

FIGURE 14. Plots of $\|\Phi(t)\|$ (blue line) and $\sum_{i=1}^{2}\sum_{l=1}^{2}\mathbf{h}_1(t)\,\bar{\mathbf{h}}_1(t)\,\varepsilon_{il}^{qq}\mathbf{RE}(t)$ (red line).

To obtain the encrypted message, it must be multiplied by 10^{38}:

$$57616395436226993457273318016337934955$$

The encrypted message m is then converted to Hex code: ''2b58839dc013b66e5c6c1d1808ad7a6b''

With key ''M11082015'', RC6 decryption algorithm can be started in EBC mode to decrypt the encrypted message.

Finally, the plaintext is obtained :

''NUTNEE''.

VI. FINDINGS AND DISCUSSION

In the past, feedback gains were resolved through trial-anderror and empirical methods. In order to speed up the synchronization, a new algorithm using IGA to solve the problem of feedback gains is proposed in this study. Figures 15a−15c show the synchronization errors $(\boldsymbol{e}_1, \boldsymbol{e}_2, \boldsymbol{e}_3)$ based on the IGA approach, which exhibited better convergence speed compared with the GA approach and the LMI approach. It is confirmed that the IGA approach can seek better feedback gains than those sought by the GA approach and the LMI approach, because the IGA's random search ability enables it to find nearly optimum solutions.

In summary, given IGA's ability to randomly search for the best solution in the entire domain, it is possible to find better feedback gains of the fuzzy controller to accelerate the error system's convergence, allowing the multiple timedelay chaotic (MTDC) systems to achieve synchronization more quickly. Furthermore, owing to the characteristics of chaos: disarray and irregularities, the chaotic systems are used to increase complexity, and then to enhance the security of cryptosystems.

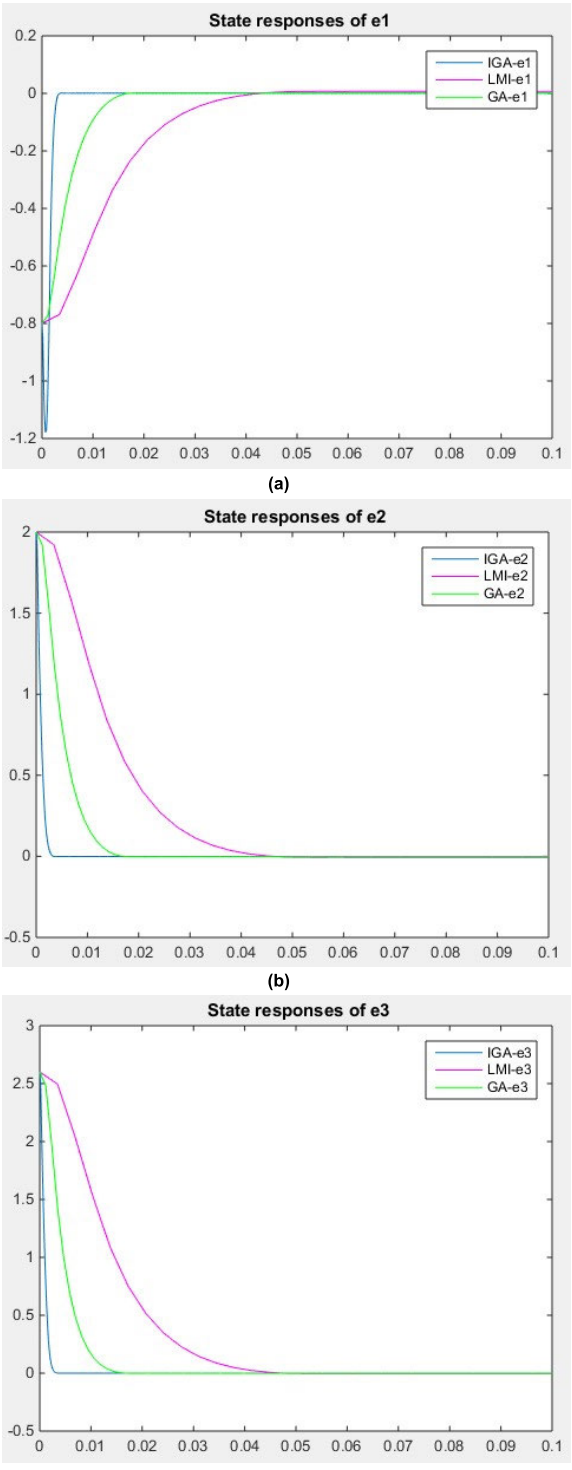

FIGURE 15. (a) State responses of e_1. (b) State responses of e_2. (c) State responses of e_3.

VII. CONCLUSION

This paper uses an IGA-based fuzzy control to propose a novel method for achieving the multiple time-delay chaotic (MTDC) systems' exponential optimal H^∞ synchronizations. This study merged the concepts of chaotic synchronization and cryptography to achieve a more secure communication system. Disarray and irregularities are the features of chaos which is used to increase complexity, and then to enhance the security of cryptosystems. However, a chaotic system can be quickly recognized in the time domain by using one of its state variables. This paper further improved the cryptosystem by combining chaotic synchronization with the RC6 encryption technique to prevent attacks. The suggested technique may safeguard the ciphertext while promoting a more secure communication system.

T-S fuzzy models were used first to simulate the MTDC systems. The influence of modeling mistakes between the MTDC systems and T-S fuzzy models was then addressed using the proposed robust fuzzy control scheme. Lyapunov's direct technique integrated a delay-dependent stability criterion to ensure that the slave system can exponentially synchronize with the master system. Then, the linear matrix inequalities (LMIs) were used to rewrite the stability criterion. A model-based fuzzy controller was created based on LMIs to exponentially stabilize the error systems. The lower and upper bounds of the search space were established based on the feedback gains obtained through the LMI technique. This allows the Improved Genetic Algorithm (IGA) to seek better feedback gains of the fuzzy controller and speed up the synchronization. Furthermore, a synthesized fuzzy controller realizes exponential synchronization and achieves the optimal H^∞ performance by minimizing the disturbance attenuation level. Based on the RC6 decryption function, the plaintext recovery from the decrypted message and the key can be achieved. Lastly, the simulation results revealed that the exponential H^∞ synchronization of the two different MTDC systems could be achieved by the designed fuzzy controller.

The future direction of this research could involve the exploration of multi-model communication systems, aiming to investigate how to integrate chaotic synchronization with other communication technologies, such as optical communication or acoustic wave communication. This integration aims to create more versatile communication systems that enhance both safety and efficiency. Additionally, these results will be applied to practical systems, including secure communication equipment and network security systems, to empirically validate the theoretical research's real-world impact.

APPENDIX

PROOF OF THEOREM 1

We define the Lyapunov function for the error system (16) as:

$$V(t) = \sum_{k=1}^{g} E^T(t)\tau_k P E(t) + \sum_{k=1}^{g}\int_0^{\tau_k} E^T(t-\pi)\psi_k E(t-\pi)d\pi \qquad (38)$$

where the weighting matrices $P = P^T > 0$ and $\psi_k = \psi_k^T > 0$. Referring to Definition 2, the initial conditions are set to be zero (i.e., $E(t) \equiv 0$ for $t \in [-\tau_{\max}, 0]$, in which $\tau_{\max}$ denotes the maximal value of time delay τ_k). We then evaluate the time derivative of $V(t)$ on the trajectories of Eq. (16) to obtain:

$$\begin{aligned}
\dot{V}(t) &= \sum_{k=1}^{g}\tau_k\left[\dot{E}^T(t)PE(t) + E^T(t)P\dot{E}(t)\right] \\
&\quad + \sum_{k=1}^{g}\left[E^T(t)\psi_k E(t) - E^T(t-\tau_k)\psi_k E(t-\tau_k)\right] \\
&= \sum_{k=1}^{g}\tau_k\left\{\sum_{i=1}^{\phi}\sum_{l=1}^{\sigma} h_i(t)\bar{h}_l(t)\left[G_{il}E(t) + \sum_{d=1}^{g}\bar{A}_{id}E(t-\tau_d)\right] + D(t) + \Phi(t)\right\}^T PE(t) \\
&\quad + \sum_{k=1}^{g}\tau_k E^T(t)P\left\{\sum_{i=1}^{\phi}\sum_{l=1}^{\sigma} h_i(t)\bar{h}_l(t) \times \left[G_{il}E(t) + \sum_{d=1}^{g}\bar{A}_{id}E(t-\tau_d)\right] + D(t) + \Phi(t)\right\} + \sum_{k=1}^{g}\left[E^T(t)\psi_k E(t) - E^T(t-\tau_k)\psi_k E(t-\tau_k)\right] \\
&= \sum_{k=1}^{g}\sum_{i=1}^{\phi}\sum_{l=1}^{\sigma} h_i(t)\bar{h}_l(t)E^T(t)\left[\tau_k G_{il}^T P + \tau_k PG_{il} + \psi_k\right]E(t) \\
&\quad + \sum_{k=1}^{g}\sum_{i=1}^{\phi}\sum_{d=1}^{g} h_i(t)\tau_k\left[E^T(t-\tau_d)\bar{A}_{id}^T PE(t) + E^T(t)P\bar{A}_{id}E(t-\tau_d)\right] \\
&\quad + \sum_{k=1}^{g}\tau_k\left[D^T(t)PE(t) + E^T(t)PD(t) + \Phi^T(t)PE(t) + E^T(t)P\Phi(t)\right] \\
&\quad - \sum_{k=1}^{g}\left[E^T(t-\tau_k)\psi_k E(t-\tau_k)\right] \qquad (39)
\end{aligned}$$

According to Lemma 1 and Eq. (39):

$$\begin{aligned}
\dot{V}(t) &\le \sum_{k=1}^{g}\sum_{i=1}^{\phi}\sum_{l=1}^{\sigma} h_i(t)\bar{h}_l(t)E^T(t)\left[bG_{il}^T G_{il} + b^{-1}\tau_k^2 P^2 + \psi_k\right]E(t) \\
&\quad + \sum_{k=1}^{g}\sum_{i=1}^{\phi}\sum_{d=1}^{g} h_i(t)\left[aE^T(t-\tau_d)\bar{A}_{id}^T\bar{A}_{id}E(t-\tau_d) + a^{-1}E^T(t)\tau_k^2P^2E(t)\right] \\
&\quad + \sum_{k=1}^{g}\left[\xi D^T(t)D(t) + \xi^{-1}E^T(t)\tau_k^2P^2E(t) + n\Phi^T(t)\Phi(t) + n^{-1}E^T(t)\tau_k^2P^2E(t)\right] \\
&\quad - \sum_{k=1}^{g}\left[E^T(t-\tau_k)\psi_k E(t-\tau_k)\right] \qquad (40) \\
&\le \sum_{k=1}^{g}\sum_{i=1}^{\phi}\sum_{l=1}^{\sigma} h_i(t)\bar{h}_l(t)E^T(t)\left[bG_{il}^T G_{il} + b^{-1}\tau_k^2 P^2 + \psi_k\right]E(t) \\
&\quad + \sum_{k=1}^{g}\sum_{i=1}^{\phi}\sum_{d=1}^{g} h_i(t)\left[aE^T(t-\tau_d)\bar{A}_{id}^T\bar{A}_{id}E(t-\tau_d) + a^{-1}E^T(t)\tau_k^2P^2E(t)\right] \\
&\quad + \sum_{k=1}^{g}\left[\xi D^T(t)D(t) + \xi^{-1}E^T(t)\tau_k^2P^2E(t)\right.
\end{aligned}$$

$$+ n\,E^T(t)R^TRE(t) + n^{-1}E^T(t)\tau_k^2P^2E(t)\Big] - \sum_{k=1}^{g}\Big[E^T(t-\tau_k)\,\psi_k E(t-\tau_k)\Big] \quad (41)$$

$$= \sum_{i=1}^{\phi}\sum_{l=1}^{\sigma} h_i(t)\bar{h}_l(t)E^T(t)\Big\{ngR^TR + \sum_{k=1}^{g}\Big[bG_{il}^TG_{il} + \psi_k + \tau_k^2P^2\Big(\xi^{-1} + n^{-1} + b^{-1} + ga^{-1}\Big)\Big]\Big\}E(t) + \sum_{k=1}^{g}\sum_{i=1}^{\phi} h_i(t)E^T(t-\tau_k)\Big[ga\bar{A}_{ik}^T\bar{A}_{ik} - \psi_k\Big]E(t-\tau_k) + \xi gD^T(t)D(t) \quad (42)$$

From Eq. (42) and Definition 2:

$$\begin{aligned}
&\dot{V}(t)E(t) - \rho^2D^T(t)D(t)\\
&\le \sum_{i=1}^{\phi}\sum_{l=1}^{\sigma} h_i(t)\bar{h}_l(t)E^T(t)\Delta_{il}E(t)\\
&\quad + \sum_{i=1}^{\phi}\sum_{k=1}^{g} h_i(t)E^T(t-\tau_k)\nabla_{ik}E(t-\tau_k)\\
&\quad + \Big(\xi g - \rho^2\Big)D^T(t)D(t)\\
&\le \sum_{i=1}^{\phi}\sum_{l=1}^{\sigma} h_i(t)\bar{h}_l(t)\lambda_{\max}(\Delta_{il})E^T(t)E(t)\\
&\quad + \sum_{i=1}^{\phi}\sum_{k=1}^{g} h_i(t)\lambda_{\max}(\nabla_{ik})E^T(t-\tau_k)E(t-\tau_k)\\
&\quad + \Big(\xi g - \rho^2\Big)D^T(t)D(t)\\
&< 0
\end{aligned} \quad (43)$$

where

$$\begin{aligned}
\Delta_{il} &\equiv \sum_{k=1}^{g} bG_{il}^TG_{il} + \sum_{k=1}^{g}\psi_k + ngR^TR + I + \sum_{k=1}^{g}\tau_k^2P^2 \times \Big(\xi^{-1} + n^{-1} + ga^{-1} + b^{-1}\Big) \quad \text{(see (20}a\text{))}\\
\nabla_{ik} &\equiv ga\bar{A}_{ik}^T\bar{A}_{ik} - \psi_k \quad \text{(see (20}b\text{))}
\end{aligned}$$

We can get the following inequality by integrating Eq. (43) from $t = 0$ to $t = \infty$:

$$V(\infty) - V(0) + \int_0^{\infty} E^T(t)E(t)dt - \rho^2\int_0^{\infty} D^T(t)D(t)dt \le 0$$

With zero initial conditions (i.e., $E(t) \equiv 0$ for $t \in [-\tau_{max}, 0]$), we have:

$$\int_0^{\infty} E^T(t)E(t)dt \le \rho^2\int_0^{\infty} D^T(t)D(t)dt$$

That is, the H^{∞} control performance (19) is realized with a prescribed attenuation ρ. Since

$$\begin{aligned}
&\sum_{k=1}^{g}\lambda_{min}(P)\tau_kE^T(t)E(t)\\
&\le \sum_{k=1}^{g} E^T(t)\tau_kPE(t)\\
&= V(t) - \sum_{k=1}^{g}\int_0^{\tau_k} E^T(t-\pi)\psi_kE(t-\pi)d\pi\\
&< V(t),
\end{aligned}$$

the following inequality can be obtained from Eq. (43):

$$\begin{aligned}
&\dot{V}(t) + E^T(t)E(t) - \rho^2D^T(t)D(t)\\
&< \sum_{i=1}^{\phi}\sum_{l=1}^{\sigma} h_i(t)\bar{h}_l(t)\left[\frac{\lambda_{max}(\Delta_{il})}{\sum_{k=1}^{g}\tau_k\lambda_{min}(P)}\right]V(t)\\
&< 0
\end{aligned} \quad (44)$$

Then, the following is obtained:

$$V(t)|_{D(t)=0} \le V(t_0)\,exp\bar{\beta}\,(t - t_0) \quad (45)$$

where

$$\bar{\beta} = \sum_{i=1}^{\phi}\sum_{l=1}^{\sigma} h_i(t)\bar{h}_l(t)\left[\frac{\lambda_{max}(\Delta_{il})}{\sum_{k=1}^{g}\lambda_{min}(P)}\right]. \quad (46)$$

Eqs. (38) and (45) show that:

$$\begin{aligned}
&\sum_{k=1}^{g}\tau_k\lambda_{min}(P)E^T(t)E(t)\\
&\le \sum_{k=1}^{g} E^T(t)\tau_kPE(t)\\
&= V(t) - \sum_{k=1}^{g}\int_{t-\tau_k}^{t} E^T(\pi)\psi_kE(\pi)d\pi\\
&< V(t_0)\,exp\bar{\beta}\,(t - t_0)\\
&\quad - \sum_{k=1}^{g}\int_{t-\tau_k}^{t} E^T(\pi)\psi_kE(\pi)d\pi\\
&< V(t_0)\,exp\bar{\beta}\,(t - t_0)
\end{aligned}$$

That is, $\|E(t)\|^2 < \frac{V(t_0)}{\sum_{k=1}^{g}\tau_k\lambda_{min}(P)}exp\bar{\beta}\,(t - t_0)$. According to Definition 1, it is concluded that:

$$\|E(t)\| \le \alpha exp\,(-\beta\,(t - t_0)) \quad \text{with } \alpha \equiv \sqrt{\frac{V(t_0)}{\sum_{k=1}^{g}\lambda_{min}(P)}} > 0 \quad (47)$$

$$\text{and } \beta = -\frac{1}{2}\bar{\beta} > 0. \quad (48)$$

Therefore, based on Definition 1, the error system (16) under the fuzzy controller (5) is exponentially stable for $D(t) = 0$.

REFERENCES

[1] H. K. Verma and R. K. Singh, "Enhancement of RC6 block cipher algorithm and comparison with RC5 & RC6," in *Proc. 3rd IEEE Int. Advance Comput. Conf. (IACC)*, Ghaziabad, India, Feb. 2013, pp. 556–561.

[2] H. E. H. Ahmed, H. M. Kalash, and O. S. F. Allah, "Encryption efficiency analysis and security evaluation of RC6 block cipher for digital images," in *Proc. Int. Conf. Electr. Eng.*, Lahore, Pakistan, Apr. 2007, pp. 1–7.

[3] H. K. Verma and R. K. Singh, "Performance analysis of RC6, twofish and rijndael block cipher algorithms," *Int. J. Comput. Appl.*, vol. 42, no. 16, pp. 1–7, Mar. 2012.

[4] N. Liu, J. Cai, X. Zeng, G. Lin, and J. Chen, "Cryptographic performance for Rijndael and RC_6 block ciphers," in *Proc. 11th IEEE Int. Conf. Anti-Counterfeiting, Secur., Identificat. (ASID)*, Xiamen, China, Oct. 2017, pp. 36–39.

[5] D. Soni, V. Tiwari, B. Kaur, and M. Kumar, "Cloud computing security analysis based on RC_6, AES and RSA algorithms in user-cloud environment," in *Proc. 1st Int. Conf. Adv. Comput. Future Commun. Technol. (ICACFCT)*, Meerut, India, Dec. 2021, pp. 269–273.

[6] Y. Liu and S. Zhang, "Fast quantum algorithms for least squares regression and statistic leverage scores," *Theor. Comput. Sci.*, vol. 657, pp. 38–47, Jan. 2017.

[7] S. B. Ramezani, A. Sommers, H. K. Manchukonda, S. Rahimi, and A. Amirlatifi, "Machine learning algorithms in quantum computing: A survey," in *Proc. Int. Joint Conf. Neural Netw. (IJCNN)*, Jul. 2020, pp. 1–8.

[8] C.-H. Yu, F. Gao, and Q.-Y. Wen, "An improved quantum algorithm for ridge regression," *IEEE Trans. Knowl. Data Eng.*, vol. 33, no. 3, pp. 858–866, Mar. 2021.

[9] W.-K. Lee, K. Jang, G. Song, H. Kim, S. O. Hwang, and H. Seo, "Efficient implementation of lightweight hash functions on GPU and quantum computers for IoT applications," *IEEE Access*, vol. 10, pp. 59661–59674, 2022.

[10] Z. Liu, C. Wu, J. Wang, and Y. Hu, "A color image encryption using dynamic DNA and 4-D memristive hyper-chaos," *IEEE Access*, vol. 7, pp. 78367–78378, 2019.

[11] H. Ren, J. Wang, and Q.-H. Wang, "An image encryption scheme of logistic modulation using computer-generated hologram and chaotic map," *J. Electr. Comput. Eng.*, vol. 2018, pp. 1–6, Apr. 2018.

[12] L. Pecora and T. Carroll, "Synchronization in chaotic systems," *Phys. Rev. Lett.*, vol. 64, no. 8, pp. 821–824, 1990.

[13] L. M. Pecora and T. L. Carroll, "Driving systems with chaotic signals," *Phys. Rev. A, Gen. Phys.*, vol. 44, no. 4, pp. 2374–2383, Aug. 1991.

[14] R. Newcomb and S. Sathyan, "An RC op amp chaos generator," *IEEE Trans. Circuits Syst.*, vol. CS-30, no. 1, pp. 54–56, Jan. 1983.

[15] K. M. Cuomo, A. V. Oppenheim, and S. H. Strogatz, "Synchronization of lorenz-based chaotic circuits with applications to communications," *IEEE Trans. Circuits Syst. II, Analog Digit. Signal Process.*, vol. 40, no. 10, pp. 626–633, Mar. 1993.

[16] K.-Y. Lian, C.-S. Chiu, T.-S. Chiang, and P. Liu, "LMI-based fuzzy chaotic synchronization and communications," *IEEE Trans. Fuzzy Syst.*, vol. 9, no. 4, pp. 539–553, Aug. 2001.

[17] Q. Liu, Y. Wang, J. Wang, and Q.-H. Wang, "Optical image encryption using chaos-based compressed sensing and phase-shifting interference in fractional wavelet domain," *Opt. Rev.*, vol. 25, no. 1, pp. 46–55, Feb. 2018.

[18] A. L. Fradkov and B. Andrievsky, "Signal transmission by sampled-time adaptive synchronization of time-varying chaotic systems," *IFAC-PapersOnLine*, vol. 55, no. 12, pp. 695–700, 2022.

[19] A. K. Mishra, S. Das, and V. K. Yadav, "Finite-time synchronization of multi-scroll chaotic systems with sigmoid non-linearity and uncertain terms," *Chin. J. Phys.*, vol. 75, pp. 235–245, Jan. 2022.

[20] M. C. Mackey and L. Glass, "Oscillation and chaos in physiological control systems," *Science*, vol. 197, no. 4300, pp. 287–289, Jul. 1977.

[21] J. H. Holland, *Adaptation in Natural and Artificial Systems: An Introductory Analysis With Applications to Biology, Control, and Artificial Intelligence*. Ann Arbor, MI, USA: Univ. Michigan, Michigan Press, 1975.

[22] D. Lee, S. Lee, J.-W. Kim, C.-G. Lee, and S.-Y. Jung, "Intelligent memetic algorithm using GA and guided MADS for the optimal design of interior PM synchronous machine," *IEEE Trans. Magn.*, vol. 47, no. 5, pp. 1230–1233, May 2011.

[23] A. Bailey, M. Ventresca, and B. Ombuki-Berman, "Genetic programming for the automatic inference of graph models for complex networks," *IEEE Trans. Evol. Comput.*, vol. 18, no. 3, pp. 405–419, Jun. 2014.

[24] G. Canisius, K. Wilson, Y. Zhang, Y. Chenhui, and H. Xin, "A genetic-based local search method for SAT problem," in *Proc. IEEE Inf. Technol., Netw., Electron. Autom. Control Conf.*, Chongqing, China, May 2016, pp. 454–458.

[25] I. Hilali-Jaghdam, A. Ben Ishak, S. Abdel-Khalek, and A. Jamal, "Quantum and classical genetic algorithms for multilevel segmentation of medical images: A comparative study," *Comput. Commun.*, vol. 162, pp. 83–93, Oct. 2020.

[26] F. H. F. Leung, H. K. Lam, S. H. Ling, and P. K. S. Tam, "Tuning of the structure and parameters of a neural network using an improved genetic algorithm," *IEEE Trans. Neural Netw.*, vol. 14, no. 1, pp. 79–88, Jan. 2003.

[27] S.-T. Pan, "Evolutionary computation on programmable robust IIR filter pole-placement design," *IEEE Trans. Instrum. Meas.*, vol. 60, no. 4, pp. 1469–1479, Apr. 2011.

[28] Z. Jin and H. Fan, "An improved immune genetic algorithm for multi-peak function optimization," in *Proc. 5th Int. Conf. Intell. Hum.-Mach. Syst. Cybern.*, vol. 1. Hangzhou, China, Aug. 2013, pp. 504–507.

[29] X. Zhang, L. Wu, and S. Cui, "An improved integral inequality to stability analysis of genetic regulatory networks with interval time-varying delays," *IEEE/ACM Trans. Comput. Biol. Bioinf.*, vol. 12, no. 2, pp. 398–409, Mar. 2015.

[30] J. Wang, "An improved genetic algorithm for web phishing detection feature selection," in *Proc. Asia Conf. Algorithms, Comput. Mach. Learn. (CACML)*, Hangzhou, China, Mar. 2022, pp. 130–134.

[31] T. Takagi and M. Sugeno, "Fuzzy identification of systems and its applications to modeling and control," *IEEE Trans. Syst. Man, Cybern.*, vol. SMC-15, no. 1, pp. 116–132, Jan. 1985.

[32] C.-P. Huang, "Admissibility and design issues for T-S fuzzy descriptor systems with perturbed derivative matrices in the rules," *IEEE Trans. Fuzzy Syst.*, vol. 30, no. 7, pp. 2574–2582, Jul. 2022.

[33] R. Vadivel and Y. H. Joo, "Finite-time sampled-data fuzzy control for a non-linear system using passivity and passification approaches and its application," *IET Control Theory Appl.*, vol. 14, no. 8, pp. 1033–1045, Apr. 2020.

[34] R. Vadivel, P. Hammachukiattikul, Q. Zhu, and N. Gunasekaran, "Event-triggered synchronization for stochastic delayed neural networks: Passivity and passification case," *Asian J. Control*, vol. 25, no. 4, pp. 2681–2698, Jul. 2023.

[35] J. Zhu, G. Wang, Y. Li, Z. Duo, and C. Sun, "Optimization of hydrogen liquefaction process based on parallel genetic algorithm," *Int. J. Hydrogen Energy*, vol. 47, no. 63, pp. 27038–27048, Jul. 2022.

[36] W.-J. Wang and C.-F. Cheng, "Stabilising controller and observer synthesis for uncertain large-scale systems by the Riccati equation approach," *IEE Proc. D, Control Theory Appl.*, vol. 139, no. 1, p. 72, 1992.

[37] Y.-J. Sun, "Exponential synchronization between two classes of chaotic systems," *Chaos, Solitons Fractals*, vol. 39, no. 5, pp. 2363–2368, Mar. 2009.

[38] R. Vadivel, S. Sabarathinam, Y. Wu, K. Chaisena, and N. Gunasekaran, "New results on T–S fuzzy sampled-data stabilization for switched chaotic systems with its applications," *Chaos, Solitons Fractals*, vol. 164, Nov. 2022, Art. no. 112741.

[39] B.-S. Chen, C.-H. Chiang, and S. K. Nguang, "Robust H_∞ synchronization design of nonlinear coupled network via fuzzy interpolation method," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 58, no. 2, pp. 349–362, Feb. 2011.

[40] S. Limanond and J. Si, "Neural network-based control design: An LMI approach," *IEEE Trans. Neural Netw.*, vol. 9, no. 6, pp. 1422–1429, Nov. 1998.

FENG-HSIAG HSIAO was born in Tainan, Taiwan, in 1960. He received the Ph.D. degree in electrical engineering from National Sun Yat-sen University, Kaohsiung, Taiwan, in 1991. He is currently a Professor with the Department of Electrical Engineering, National University of Tainan, Tainan. His research interests include fuzzy control, neural networks, large-scale control, and the dither problem.

SHOU-WEN CHANG was born in Kaohsiung, Taiwan, in 1998. He received the B.S. degree in electrical engineering from Yuan Ze University, in 2020. He is currently pursuing the M.S. degree with the Department of Electrical Engineering, National University of Tainan, Tainan, Taiwan. He has been a Research Assistant with the Intelligent Control Laboratory, National University of Tainan.