IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received November 24, 2021, accepted December 17, 2021, date of publication December 21, 2021,
date of current version January 5, 2022.

Digital Object Identifier 10.1109/ACCESS.2021.3137356

Applying 3DES to Chaotic Synchronization Cryptosystems

FENG-HSIAG HSIAO
Department of Electrical Engineering, National University of Tainan, Tainan 70005, Taiwan
e-mail: fhhsiao@mail.nutn.edu.tw

This work was supported by the Ministry of Science and Technology of Taiwan under Grant 109-2221-E-024-006.

ABSTRACT The triple data encryption standard (3DES) has played a key role in the field of data encryption over the past few decades. However, the ciphertext's security is decreased by the meet-in-the-middle attack. Accordingly, we propose a systematic design methodology combining chaotic synchronization with 3DES to conduct double encryption. The encryption method not only increases the strength of the communications system but also effectively protects the encrypted message (ciphertext). The conventional genetic algorithm (GA) has flaws in premature convergence and local search. While the methods of improving the GA performance have been explored, we adopted an improved genetic algorithm (IGA) in this work due to its better performance in the light of globalization and convergence rate. The IGA-based observer not only realizes the exponential synchronization but also minimizes the disturbance attenuation level to get optimal H^{∞} performance simultaneously. In the end, an example with numerical simulations is provided to demonstrate the effectiveness of this study.

INDEX TERMS Double encryption, chaotic synchronization, exponential synchronization, improved genetic algorithm, triple data encryption algorithm.

I. INTRODUCTION

In time-delay systems, stability and stabilization are particularly important factors and have drawn significant attention recently [1]. Engineering systems, such as electronic networks and hydraulic frequently include time delays. In particular, a time-delay factor tends to complicate the analysis. Numerous studies have hence concentrated on developing suitable methods of stability. Stability criteria for time-delay systems have traditionally been treated as delay-dependent or delay-independent conditions. Therefore, 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 [2] first demonstrated the chaotic phenomena in time-delay systems. Chaos is an apparently random behavior in a deterministic system characterized by sensitive dependence on initial conditions, and chaotic phenomena can result in irregular performance [3]. Owing to these properties, scientists have interests in chaos in different research domains [4]. Since two decades, researchers have established a strong relationship between chaos and cryptography [5], [6]. Furthermore, chaotic synchronization has been applied in the area of engineering science, physics, and particularly in communication security.

Pecora and Carroll [7] proposed the purpose of chaotic synchronization in 1990 to control one chaotic system to follow another. According to this notion, multiple synchronization methods have progressed over the past three decades. Chaotic synchronization has applications in numerous research fields, especially in secure communication [8]–[11]. Lately, many different theoretical and experimental control methods (such as fuzzy control, observer-based control, and adaptive control) have been attempted to synchronize the chaotic systems [12]–[14].

The problem of noise is unavoidable when the chaotic properties in observational time series are analyzed [15]. The disturbance or noise may lead to instability and negatively affect the performance of chaotic systems. Hence, research on reducing the effects of exterior disturbances in the synchronization process is needed [16]–[18]. For example, in the past few years, the H^{∞} control has been applied in the synchronization of chaotic systems [17]–[21], and the problem relating to H^{∞} synchronization for time-delay chaotic systems has been widely explored [18], [22]–[24]. Therefore, this work carried out the exponential synchronization of

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

multiple time-delay chaotic (MTDC) systems, and decayed the influence of exterior disturbances on the performance of control to a minimum.

Genetic algorithm (GA), introduced by Holland in 1975 [25], is an interesting field for computer scientists. Owing to its flexibility and robustness, GA has attracted significant attention. By working with a population of solutions, it can search for many local minima, and thereby raise the probability of finding the global minimum [26]. Some modern studies have successfully reported applications of GA in control systems [27]–[29]. GA has the capability of random searches for near-optimal solutions, therefore, the upper and lower bounds of the search region can be set (in view of the feedback gains by means of LMI approach) so that the GA will hence search for better feedback gains to accelerate the synchronization process. Nevertheless, the conventional GA has shortcomings of premature convergence and local search. Many studies have explored methods of the improving GA performance [30]–[33]. In this work, we adopted the improved genetic algorithm (IGA) due to its better performance considering globalization and convergence rate.

The National Institute of Standards and Technology (NIST) adopted a data encryption standard (DES) in 1977 [34], [35], which is a grouped 64-bit data decryption and encryption with the same structure but uses different order keys. However, each 8-bit is employed as parity check and it can be neglected, and the keys are generally expressed as 64-bit. Accordingly, the length of the keys is 56-bit [36]. Currently, DES decryption can be broken by the brute-force attack within a short time at a reasonable cost [37], [38]. Hence, DES has been replaced by 3DES [39], [40] with three independent keys (three 56-bit DES keys). Nevertheless, owing to the "meet in the middle" attack [41], the effective security of 3DES has only 112 bits.

This study hence combines chaotic synchronization with 3DES to implement double encryption to enhance the overall security and effectively protect the encrypted message. First, three keys are used via the 3DES encryption function to obtain the encrypted message (ciphertext) and employed to accomplish double encryption by chaotic synchronization. Then, we propose an effective way via the IGA-based fuzzy observer method to achieve the exponential optimal H^{∞} synchronization of two MTDC systems. Subsequently, we derived a delay-dependent exponential stability criterion according to the Lyapunov approach to warrant the exponential stability of the error system between the slave and the master systems. After this, we reformulated the stability conditions into LMIs. Based on LMIs, we could synthesize a model-based fuzzy observer to exponentially stabilize the error system. Moreover, the trajectories of the slave systems can more quickly approach those of the master systems through IGA, and the effect of exterior disturbances on the control performance can be decayed to a minimum.

II. PROBLEM FORMULATION

We considered a master-slave configuration with two multiple time-delay chaotic (MTDC) systems in this study. The dynamics of the master system (N_m) and the slave system (N_s) are depicted below:

$$N_m : \dot{X}(t) = f(X(t)) + \sum_{k=1}^{g} H_k(X(t-\tau_k)) \tag{2.1}$$

$$N_s : \dot{\hat{X}}(t) = \hat{f}(\hat{X}(t)) + \sum_{k=1}^{g} \hat{H}_k(\hat{X}(t-\tau_k)) + D(t) \tag{2.2}$$

where $\tau_k(k = 1, 2, \cdots, g)$ denotes the time delays, $f(\cdot)$, $H_k(\cdot)$, $\hat{f}(\cdot)$ and $\hat{H}_k(\cdot)$ denote the nonlinear vector-valued functions, and $D(t)$ denotes the exterior disturbance.

This section demonstrates that at first, three keys and the 3DES encryption function are utilized to encrypt the plaintext (original message) to generate the ciphertext (encrypted message), and then it is re-encrypted by chaotic synchronization to carry out the double encryption. Afterward, a T-S fuzzy model is constructed to approximate the MTDC system.

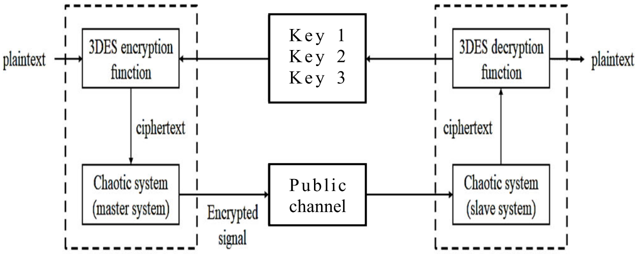


FIGURE 1. Chaotic synchronization cryptosystem.

Fig. 1 shows a chaotic synchronization cryptosystem which consists of a decrypter and an encrypter. First, the ciphertext (encrypted message) is acquired by three keys (key 1, key 2, and key 3) and the plaintext via the 3DES encryption function. It is then forwarded to the master system and transformed into the encrypted signal by chaotic masking. Next, the encrypted signal is transmitted to the slave system via the public channel and is filtered by the chaotic system to get the ciphertext. Finally, after decrypting the ciphertext by three keys, it is then transformed to the plaintext by means of the 3DES decryption function.

A. 3DES CRYPTOSYSTEM

DES is a symmetric encryption algorithm that requires a key and a plaintext as two inputs. The key length of DES is generally expressed as 64 bits, but each 8-bit can be ignored which is used as a parity check [36]. Fig. 2 shows a block diagram of DES and parts A∼D give the details [42]–[44].

1) INITIAL PERMUTATION

The encryption begins by shuffling the plaintext via the initial permutation (IP) according to the scheme below (Figure 2).

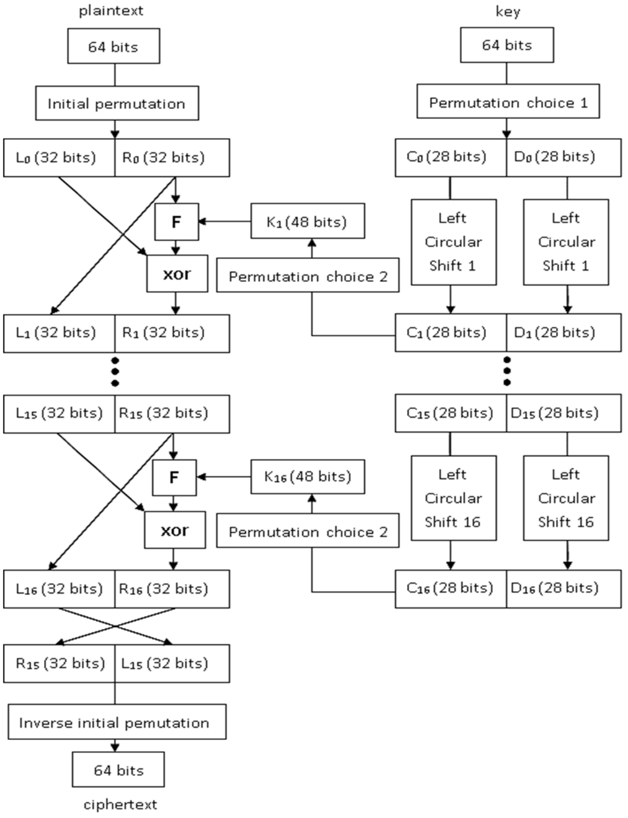


FIGURE 2. The structure of the data encryption standard (DES).

TABLE 1. Initial permutation of the plaintext.

58	50	42	34	26	18	10	2
60	52	44	16	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

Based on the permutation mentioned in Table 1, the plaintext was divided into left side L_0 (32 bits) and right side R_0 (32 bits).

2) DATA ENCRYPTION STANDARD ENCRYPTION SCHEME

DES encryption process mathematical formula is described as:

$$L_b = R_{b-1} \tag{2.3}$$

$$R_b = L_{b-1} \oplus f(R_{b-1}, K_b) \tag{2.4}$$

where $b = 1, 2 \ldots, 16$; the notation $\oplus$ is the XOR operation; the length of K_b is 48-bit, which is calculated by the private key and each round is updated according to key schedule (shown in the next part **C**). $f(\cdot)$ is the cipher function (described in part D), the input for 32-bit (R_{b-1}) and 48-bit (K_b), then yields a block of 32-bit as the output.

At the end of 16 rounds of calculation, it creates a 64-bit data set. The left 32-bit is considered as R_{16} and the right 32-bit is L_{16}. After the two sides merge, the 64-bit ciphertext $R_{16}L_{16}$ is achieved by rearranging the data through inverse initial permutation, the obtained permutation (Table 2) is the inverse permutation.

TABLE 2. Inverse permutation.

40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25

3) KEY SCHEDULE

(a) Permutated Choice 1 (PC1): Permute a 64-bit input to two 28-bit outputs.

(b) Permutated Choice 2 (PC2): Permute a 56-bit input to 48-bit output.

(c) Left Shifts: Performs a bit-wise operation on the input, shifting it to the left.

First, the 64-bit private key is permuted with PC1, leading to two 28-bit results denoted as T_0 and U_0, respectively. The permutation is mentioned in Table 3.

Next, we use the following formula to calculate K_b in each round:

$$\begin{aligned} T_b &= LS_b(T_{b-1}) \\ U_b &= LS_b(U_{b-1}) \\ K_b &= PC2(T_bU_b) \end{aligned} \tag{2.5}$$

where LS_b is the left circular shift operation, and the specific number of bits per shift from the following table is determined by Table 4.

After splicing T_b and U_b, the 56-bit block is obtained, and by using PC2 it is then permuted into 48-bit as the K_b of this round. The PC2 is shown in Table 5.

From the above, the process of key schedule is demonstrated in Fig. 3.

TABLE 3. PC1 to T_0 and U_0.

57	49	41	33	25	17	9
1	58	50	42	34	26	18
10	2	59	51	43	35	27
19	11	3	60	52	44	36

63	55	47	39	31	23	15
7	62	54	46	38	30	22
14	6	61	53	45	37	29
21	13	5	28	20	12	4

TABLE 4. Left circular shift operation 1∼16.

b	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
LS_b	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

TABLE 5. PC2.

14	17	11	24	1	5
3	28	15	6	21	10
23	19	12	4	26	8
16	7	27	20	13	2
41	52	31	37	47	55
30	40	51	45	33	48
44	49	39	56	34	53
46	42	50	36	29	32

4) CIPHER FUNCTION

(a) Expand permutation: the input is 32-bit and the output is 48-bit.

(b)Substitution-box(S_b): the input is 6-bit and the output is 4-bit.

Fig. 4 shows the process of cipher function. First, from (2.3), a 48-bit R_{b-1} is obtained through the expand permutation, which is determined as below (Table 6):

Next, from (2.4), we set 6-bit as a group, defined as:

$$B_1B_2\cdots B_8$$

for each B_b, the corresponding S-box shown in [44] was used to permute and splice the results together. The 32-bit result is demonstrated as:

$$S_1(B_1)S_2(B_2)\cdots S_8(B_8)$$

The cipher function permutation yields a 32-bit output from a 32-bit input by permuting the bits of the input block. Such a function is defined in Table 7.

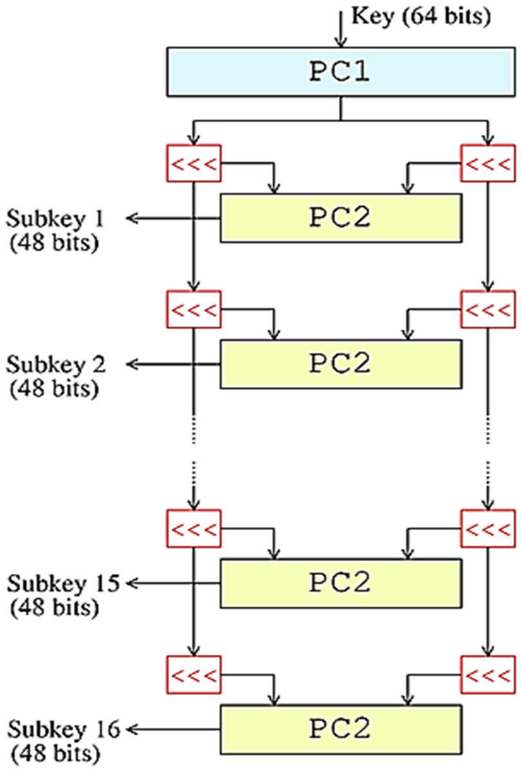


FIGURE 3. Key schedule of the data encryption standard (DES).

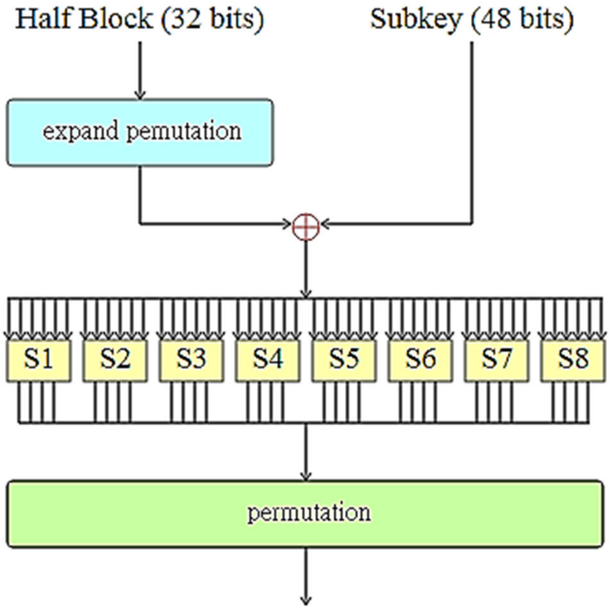


FIGURE 4. The process of cipher function.

TABLE 6. Expand permutation.

32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

TABLE 7. Cipher function permutation.

16	7	20	21	29	12	28	17
1	15	23	26	5	18	31	10
2	8	24	14	32	27	3	9
19	13	30	6	22	11	4	25

Therefore, the result of the encryption function $f(\cdot)$ is as below:

$$P(S_1(B_1)S_2(B_2)\cdots S_8(B_8))$$

However, the key length of DES is too short. Accordingly, 3DES is designed to raise the key length and enhance the strength of encryption. Here, 3DES is utilized to decrypt and encrypt the three DESs with three different keys. This work presents the cipher block chaining (CBC) mode which uses three 64 bits private keys $(\kappa_1, \kappa_2, \kappa_3)$ and a non-secret 64 bits IV (initializing vector) to encrypt n64 bits blocks plaintext $(P, P_2, \ldots, P_n)$ to produce n64 bits blocks ciphertext $(\Upsilon_1, \Upsilon_2, \ldots, \Upsilon_n)$ [34]. The encryption scheme of 3DES is given as below:

$$\Upsilon = E_{\kappa 3}(D_{\kappa 2}(E_{\kappa 1}(P))) \tag{2.6}$$

where Υ is ciphertext, D_κ is conducted by DES decryption with κ, E_κ is conducted by DES encryption with κ, and P is the plaintext.

The corresponding scheme of decryption is shown below:

$$P = D_{\kappa 1}(E_{\kappa 2}(D_{\kappa 3}(\Upsilon))) \tag{2.7}$$

Fig. 5 shows the CBC mode of 3DES.

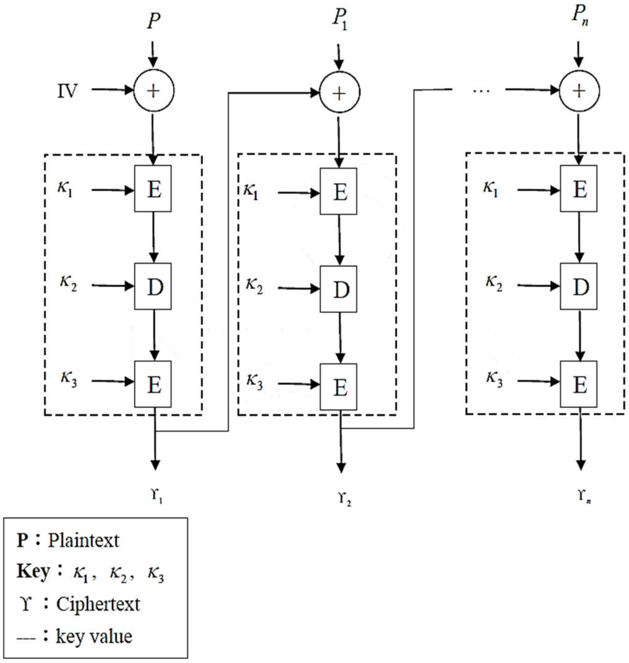


FIGURE 5. Cipher block chaining mode of the three data encryption standard (3DES).

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

A little more than three decades ago, Takagi and Sugeno [45] pioneered a fuzzy dynamical model to express the relations of a local linear input/output nonlinear system and employed IF-THEN rules to describe this dynamic model. To deal with the problem of synchronization of MTDC systems, the rules are used in this study.

The i th rule of the T-S fuzzy model for the master system is given below:

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

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

where $M_{i\eta}(\eta = 1, 2, \cdots, \delta)$ are the fuzzy sets, and $x_1(t) \sim x_\delta(t)$ are the premise variables; A_i and $\bar{A}_{ik}$ are constant matrices with appropriate dimensions; $i = 1, 2, \cdots, \phi$ and ϕ denotes the number of IF-THEN rules.

We infer the final state of this fuzzy dynamic model according to Eq. (2.8):

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

$$= \sum_{i=1}^{\phi} h_i(t)\{A_i X(t) + \sum_{k=1}^{g} \bar{A}_{ik} X(t-\tau_k)\} \tag{2.8}$$

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

Similarly, the ℓth rule of the T-S fuzzy model for the slave system is given below:

Rule ℓ: IF $\hat{x}_1(t)$ is $\hat{M}_{\ell 1}$ and $\cdots$ and $\hat{x}_\delta(t)$ is $\hat{M}_{\ell\delta}$
THEN $\dot{\hat{X}}(t) = \hat{A}_\ell \hat{X}(t) + \sum_{k=1}^{g} \hat{\hat{A}}_{\ell k}\hat{X}(t-\tau_k) + D(t)$

where $\hat{M}_{\ell\eta}(\eta = 1, 2, \cdots, \delta)$ are the fuzzy sets, $\hat{x}_1(t) \sim \hat{x}_\delta(t)$ are the premise variables, $\hat{A}_\ell$ and $\hat{\hat{A}}_{\ell k}$ are constant matrices with appropriate dimensions, $\ell = 1, 2, \cdots, \sigma$ and σ is the number of IF-THEN rules.

We infer the final state of this fuzzy dynamic model according to Eq. (2.9):

$$\dot{\hat{X}}(t) = \frac{\sum_{\ell=1}^{\sigma} \hat{w}_\ell(t)\left[\hat{A}_\ell \hat{X}(t) + \sum_{k=1}^{g} \hat{\hat{A}}_{\ell k}\hat{X}(t-\tau_k) + D(t)\right]}{\sum_{\ell=1}^{\sigma} \hat{w}_\ell(t)}$$
$$= \sum_{\ell=1}^{\sigma} \hat{h}_\ell(t)\{\hat{A}_\ell \hat{X}(t) + \hat{\hat{A}}_{\ell k}\hat{X}(t-\tau_k)\} + D(t) \quad (2.9)$$

where $\hat{w}_\ell(t) \equiv \prod_{\eta=1}^{\delta} \hat{M}_{\ell\eta}(\hat{x}_\eta(t))$, and $\hat{M}_{\ell\eta}(\hat{x}_\eta(t))$ is the grade of membership of $\hat{x}_\eta(t)$ in $\hat{M}_{\ell\eta}$. In addition, $\hat{h}_\ell(t) \equiv \frac{\hat{w}_\ell(t)}{\sum_{\ell=1}^{\sigma}\hat{w}_\ell(t)}$, and $\sum_{\ell=1}^{\sigma} \hat{h}_\ell(t) = 1$ for all t.

C. FUZZY OBSERVER

We assumed that the dynamic fuzzy model of the slave system is observable for the fuzzy observer design. First, the fuzzy observer is designed on the basis of the doublets $(\hat{A}_\ell, C)$ below:

Observer Rule ℓ: IF $\hat{x}_1(t)$ is $\bar{M}_{\ell 1}$ and $\cdots$ and $\hat{x}_\delta(t)$ is $\bar{M}_{\ell\delta}$
THEN

$$\dot{\hat{X}}(t) = \hat{A}_\ell \hat{X}(t) + \sum_{k=1}^{g} \hat{\hat{A}}_{\ell k}\hat{X}(t-\tau_k) + Z_\ell(Y(t) - \hat{Y}(t)) + D(t)$$
$$\hat{Y}(t) = C\hat{X}(t)$$

where $\bar{M}_{\ell\eta}(\eta = 1, 2, \cdots, \delta)$ are the fuzzy sets, and Z_ℓ is the observer gain, $\ell = 1, 2, \cdots, m$; m is the number of IF-THEN fuzzy observer rules; $Y(t)$ and $\hat{Y}(t)$ denote the final outputs of the master system and the slave system, respectively.

Therefore, we infer the overall fuzzy observer below:

$$\dot{\hat{X}}(t) = \sum_{\ell=1}^{m} \hat{h}_\ell(t)\{\hat{A}_\ell \hat{X}(t) + \sum_{k=1}^{g} \hat{\hat{A}}_{\ell k}\hat{X}(t-\tau_k)\} + Z_\ell(Y(t) - \hat{Y}(t)) + D(t)$$
$$\hat{Y}(t) = C\hat{X}(t) \quad (2.10)$$

Formerly, solving the observer gains, Z_ℓ $(\ell = 1, 2, \cdots, m)$ was based on trial-and-error and experience. It would hence be helpful to develop an effective tool for solving proper observer gains. This study applies the IGA mentioned in the next subsection to create a new algorithm for solving observer gains.

D. IMPROVED GENETIC ALGORITHM

GA works with a population of solutions to seek many local minima, thus raising the probability of finding the global minimum [25]. Nevertheless, the conventional GA has shortcomings of premature convergence and local search. This study adopts IGA, whose superiority over the standard GA was demonstrated by Leung *et al.* [30] for the GA-based observer gain design to ameliorate the performance of the proposed method. The key point of IGA is that the chromosomes after crossover are placed in the boundary and central areas of the search domain in most cases. This leads to that the next generation will be more likely to seek a globally optimal solution. The improved crossover is presented in Eqs. (2.11) to (2.16) as [30], [46]:

$$os_c^1 = [os_1^1 os_2^1 \cdots os_{no\_vars}^1] = \frac{P_1 + P_2}{2} \quad (2.11)$$
$$os_c^2 = [os_1^2 os_2^2 \cdots os_{no\_vars}^2] = P_{\max}(1-w) + \max(P_1, P_2)w \quad (2.12)$$
$$os_c^3 = [os_1^3 os_2^3 \cdots os_{no\_vars}^3] = P_{\min}(1-w) + \min(P_1, P_2)w \quad (2.13)$$
$$os_c^4 = [os_1^4 os_2^4 \cdots os_{no\_vars}^4] = \frac{(P_{\max} + P_{\min})(1-w) + (P_1 + P_2)w}{2} \quad (2.14)$$

where

$$P_{\max} = [para_{\max}^1\, para_{\max}^2 \cdots para_{\max}^{no\_vars}] \quad (2.15)$$
$$P_{\min} = [para_{\min}^1\, para_{\min}^2 \cdots para_{\min}^{no\_vars}] \quad (2.16)$$

where P_1 and P_2 are the two chromosomes selected from the parent, $os_c^1 \sim os_c^4$ denote 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 of the genes in the two chromosome P_1 and P_2. $para_{\min}^\vartheta, para_{\max}^\vartheta$ are the lower and upper bounds of the ϑth genes in the search domain. Parameter $w \in [0, 1]$ is arbitrarily chosen. These two new chromosomes scattered in the central region of the search area are shown in equations (2.11) and (2.14), while (2.12) and (2.13) create two new chromosomes scattered in the boundary area.

We define the fitness function as follows:

$$Fit(\Lambda) = \frac{1}{1 + \sum_{t=0}^{t_f}\sum_{\eta=1}^{\delta}\left|e_\eta^\Lambda(t)\right|} \quad (2.17)$$

where $Fit(\Lambda)$ and $e_\eta^\Lambda(t)$ are the fitness value and the error, respectively, of the Λth chromosome in a population.

III. STABILITY ANALYSIS AND CHAOTIC SYNCHRONIZATION VIA FUZZY OBSERVER

This work inspects the synchronization of multiple time-delay chaotic (MTDC) systems under the influence of a modeling error in this section. In the following subsections, we depict the scheme of exponential synchronization for the MTDC systems.

A. THE MASTER-SLAVE SYSTEM

According to Section II, we depict the T-S fuzzy models of the master system with the encrypted message (ciphertext) $\boldsymbol{\imath}(\cdot)$ and the slave system under fuzzy observer as:

$$\begin{aligned}
\text{Master: } \dot{X}(t) &= \sum_{i=1}^{u} h_{\,i}(t)\{A_i X(t) + \sum_{k=1}^{g} \bar{A}_{\,ik} X(t-\tau_k)\} + \boldsymbol{\imath}(\cdot) \\
Y(t) &= CX(t) \\
\text{Slave: } \dot{\hat{X}}(t) &= \sum_{\ell=1}^{m} \hat{h}_\ell(t)[\hat{A}_\ell \hat{X}(t) + \sum_{k=1}^{g} \hat{\bar{A}}_{\ell k} \hat{X}(t-\tau_k)] \\
&\quad + Z_\ell(Y(t) - \hat{Y}(t)) + D(t) \\
Y(t) &= CX(t)
\end{aligned}$$

where $X(t)$ and $\hat{X}(t)$ are the state vectors; $Y(t)$ and $\hat{Y}(t)$ are the output vectors. $D(t)$ denotes the exterior disturbance, Z_ℓ denotes the observer gain.

B. THE ERROR SYSTEMS

According to Eqs (2.1) and (2.2), the synchronization error is defined 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 with the fuzzy observer (2.10) can be depicted as:

$$\begin{aligned}
\dot{E}(t) &= \hat{\Psi} + D(t) - \Psi \\
&= \sum_{i=1}^{u}\sum_{\ell=1}^{m} h_i(t)\left\{(A_{\,i} - Z_\ell C)\,E(t) + \sum_{k=1}^{g} \bar{A}_{ik} E(t-\tau_k)\right\} \\
&\quad + D(t) + \Phi(t)
\end{aligned}$$

where

$$\begin{aligned}
\hat{\Psi} &\equiv \hat{f}(\hat{X}(t)) + \sum_{k=1}^{g} \hat{H}_k(\hat{X}(t-\tau_k)) + Z_\ell(Y(t) - \hat{Y}(t)), \\
\Psi &\equiv f(X(t)) + \sum_{k=1}^{g} H_k(X(t-\tau_k)) + \boldsymbol{\imath}(\cdot) \text{ and} \\
\Phi(t) &\equiv \hat{\Psi} - \Psi - \left\{\sum_{i=1}^{u}\sum_{\ell=1}^{m} h_i(t)[(A_{\,i} - Z_\ell C)E(t)\right. \\
&\quad \left. + \sum_{k=1}^{g} \bar{A}_{ik} E(t-\tau_k)]\right\}.
\end{aligned}$$

Assuming that there exists a bounding matrix $\varepsilon^{qq}_{i\,l} R$ such that:

$$\|\Phi(t)\| \le \left\| \sum_{i=1}^{u}\sum_{\ell=1}^{m} h_i(t)\,\varepsilon^{qq}_{il} RE(t) \right\| \tag{3.2}$$

where $\|\varepsilon_{\,il}\| \le 1$, for $i = 1,\ 2, \cdots,\ u; l = 1,\ 2, \cdots, m$ and R denotes the specified structured bounding matrix. From (3.2), we have

$$\begin{aligned}
\Phi^T(t)\Phi(t) &\le \sum_{i=1}^{u}\sum_{\ell=1}^{m} h_i(t)\,\|RE(t)\| \\
&\quad \times \left\|\varepsilon^{qq}_{\,i\ell}\right\| \sum_{i=1}^{u}\sum_{\ell=1}^{m} h_i(t)\left\|\varepsilon^{qq}_{\,i\ell}\right\| \|RE(t)\| \\
&\le [RE(t)]^T [RE(t)]
\end{aligned} \tag{3.3}$$

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

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

We propose a delay-dependent criterion in this subsection to ensure the exponential stability of the error system depicted in (3.1). Prior to inspecting the stability of the error system, some lemma and definitions are provided.

Lemma 1 [47]: For the real matrices A and B with appropriate dimension:

$$A^T B + B^T A \le \lambdabar A^T A + \lambdabar^{-1} B^T B$$

where $\lambdabar$ is a positive constant.

Definition 1 [48], [49]: If there exist two positive numbers α and β, the slave system (2.2) can exponentially synchronize with the master system (2.1) (that is to say the error system (3.1) is exponentially stabilized) so that the synchronization error satisfies:

$$\|E(t)\| \le \alpha exp(-\beta(t-t_0)), \forall t \ge 0$$

where the positive number β is the exponential convergence rate.

Definition 2 [17]: If the following conditions are satisfied, the master system (2.1) and slave system (2.2) are said to be in exponential H^∞ synchronization:

(i). With zero disturbance (that is, $D(t) = 0$), the error system (3.1) under the fuzzy observer (2.10) is exponentially stable.

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

$$\Theta(E(t), D(t)) = \int_0^\infty E^T(t)E(t)dt - \rho^2 \int_0^\infty D^T(t)D(t)dt \le 0 \tag{3.4}$$

in which the parameter ρ denotes the disturbance attenuation level or the H^∞-norm bound. If the minimum ρ is found to meet the aforementioned conditions (that is, the error system can exclude the exterior disturbance as strongly as possible), the fuzzy observer (2.10) is an optimal H^∞ synchronizer.

Theorem 1: For given positive constants a, b, ξ, and n, if there exist two symmetric positive definite matrices ψ_k and P, so that the following inequalities hold, then the exponential H^∞ synchronization with the disturbance attenuation ρ is ensured via the fuzzy observer (2.10):

$$\Delta_{i\ell} \ \equiv b(A_{\,i} - Z_\ell\ C)^T(A_{\,i} - Z_\ell\ C) + \sum_{k=1}^{g} \psi_k + ngR^T R + I$$

$$+\sum_{k=1}^{g}\tau_k^2P^2(b^{-1}+\xi^{-1}+n^{-1}+ga^{-1})<0 \quad (3.5a)$$

$$\nabla_{ik}\equiv ga\bar{A}_{ik}^T\bar{A}_{ik}-\psi_k<0 \quad (3.5b)$$

$$\rho>\sqrt{\xi g} \quad (3.5c)$$

where $G_{il}\equiv A_i-Z_\ell C$, for $i=1,\ 2,\cdots,\ u; k=1,2,\cdots,g$ and $\ell=1,2,\cdots,m$.

Proof: The Lyapunov function for the error system (3.1) is defined as:

$$V(t)=\sum_{k=1}^{g}E^T(t)\tau_kPE(t)+\sum_{k=1}^{g}\int_{t-\tau_k}^{t}E^T(\pi)\psi_kE(\pi)d\pi \quad (3.6)$$

where the weighting matrices $P=P^T>0$ and $\psi_k=\psi_k^T>0$. This study then evaluates the time derivative of $V(t)$ on the trajectories of (3.1) to obtain:

$$\begin{aligned}\dot{V}(t)&=\sum_{k=1}^{g}\tau_k\left[\dot{E}^T(t)PE(t)+E^T(t)P\dot{E}(t)\right]\\&\quad+\sum_{k=1}^{g}\left[E^T(t)\psi_kE(t)-E^T(t-\tau_k)\psi_kE(t-\tau_k)\right]\\&=\sum_{k=1}^{g}\tau_k\left\{\sum_{i=1}^{u}\sum_{\ell=1}^{m}h_i(t)\left[(A_i-Z_\ell C)E(t)\right.\right.\\&\quad\left.\left.+\sum_{d=1}^{g}\bar{A}_{id}E(t-\tau_d)\right]+D(t)+\Phi(t)\right\}^TPE(t)\\&\quad+\sum_{k=1}^{g}\tau_kE^T(t)P\left\{\sum_{i=1}^{u}\sum_{\ell=1}^{m}h_i(t)\ \left[(A_i-Z_\ell C)E(t)\right.\right.\\&\quad\left.\left.+\sum_{d=1}^{g}\bar{A}_{id}E(t-\tau_d)+D(t)+\Phi(t)\right]\right\}\\&\quad+\sum_{k=1}^{g}\left[E^T(t)\psi_kE(t)-E^T(t-\tau_k)\psi_kE(t-\tau_k)\right]\\&=\sum_{k=1}^{g}\sum_{i=1}^{u}\sum_{\ell=1}^{m}h_i(t)E^T(t)\left[\tau_k(A_i-Z_\ell C)^TP\right.\\&\quad\left.+\tau_kP(A_i-Z_\ell C)+\psi_k\right]E(t)\\&\quad+\sum_{k=1}^{g}\sum_{i=1}^{u}\sum_{d=1}^{g}h_i(t)\left[E^T(t-\tau_d)\tau_k\bar{A}_{id}^TPE(t)\right.\\&\quad\left.+E^T(t)\tau_kP\bar{A}_{id}E(t-\tau_d)\right]\\&\quad+\sum_{k=1}^{g}\left[D^T(t)\tau_kPE(t)+E^T(t)\tau_kPD(t)\right.\\&\quad\left.+\Phi^T(t)\tau_kPE(t)+E^T(t)\tau_kP\Phi(t)\ \right]\\&\quad-\sum_{k=1}^{g}\left[E^T(t-\tau_k)\psi_kE(t-\tau_k)\right] \quad (3.7)\end{aligned}$$

According to Lemma 1 and Eq. (3.7):

$$\begin{aligned}\dot{V}(t)&\leq\sum_{k=1}^{g}\sum_{i=1}^{u}\sum_{\ell}^{m}h_iE^T(t)[b(A_i-Z_\ell C)^Tb(A_i-Z_\ell C)\\&\quad+b^{-1}\tau_k^2P^2+\psi_k]E_T\\&\quad+\sum_{k=1}^{g}\sum_{i=1}^{u}\sum_{d=1}^{g}h_i(t)\left[aE^T(t-\tau_d)\bar{A}_{id}^T\bar{A}_{id}E(t-\tau_d)\right.\\&\quad\left.+a^{-1}E^T(t)\tau_k^2P^2E(t)\right]\\&\quad+\sum_{k=1}^{g}\left[\xi D^T(t)D(t)+\xi^{-1}E^T(t)\tau_k^2P^2E(t)\right.\\&\quad\left.+n\,\Phi^T(t)\Phi(t)+n^{-1}E^T(t)\tau_k^2P^2E(t)\right]\\&\quad-\sum_{k=1}^{g}\left[E^T(t-\tau_k)\psi_kE(t-\tau_k)\right] \quad (3.8)\\&\leq\sum_{k=1}^{g}\sum_{i=1}^{u}\sum_{\ell}^{m}h_iE^T(t)[b(A_i-Z_\ell C)^Tb(A_i-Z_\ell C)\\&\quad+b^{-1}\tau_k^2P^2+\psi_k]E_T\\&\quad+\sum_{k=1}^{g}\sum_{i=1}^{u}\sum_{d=1}^{g}h_i(t)\left[aE^T(t-\tau_d)\bar{A}_{id}^T\bar{A}_{id}E(t-\tau_d)\right.\\&\quad\left.+a^{-1}E^T(t)\tau_k^2P^2E(t)\right]\\&\quad+\sum_{k=1}^{g}\left[\xi D^T(t)D(t)+\xi^{-1}E^T(t)\tau_k^2P^2E(t)\right.\\&\quad+nE^T(t)R^TRE(t)\\&\quad\text{(byEq(3.3))}\\&\quad\left.+n^{-1}E^T(t)\tau_k^2P^2E(t)\right]\\&\quad-\sum_{k=1}^{g}\left[E^T(t-\tau_k)\psi_kE(t-\tau_k)\right] \quad (3.9)\\&=\sum_{i=1}^{u}\sum_{\ell=1}^{m}h_i(t)E^T(t)\left[b(A_i-Z_\ell C)^T(A_i-Z_\ell C)\right.\\&\quad+b^{-1}\sum_{k=1}^{g}\tau_k^2P^2+\sum_{k=1}^{g}\psi_k+ngR^TR\\&\quad\left.+\sum_{k=1}^{g}\tau_k^2P^2(\xi^{-1}+n^{-1}+ga^{-1})\right]E(t)\\&\quad+\sum_{k=1}^{g}\sum_{i=1}^{u}h_i(t)E^T(t-\tau_k)\left[ga\bar{A}_{ik}^T\bar{A}_{ik}-\psi_k\right]E(t-\tau_k)\\&\quad+\xi gD^T(t)D(t) \quad (3.10)\end{aligned}$$

From (3.10):

$$\begin{aligned}&\dot{V}(t)+E^T(t)E(t)-\rho^2D^T(t)D(t)\\&\leq\sum_{i=1}^{u}\sum_{\ell=1}^{m}h_i(t)\,E^T(t)\left[b(A_i-Z_\ell C)^T(A_i-Z_\ell C)\right.\end{aligned}$$

$$
\begin{aligned}
&+b^{-1}\sum_{k=1}^{g}\tau_k^2P^2+\sum_{k=1}^{g}\psi_k\\
&+ngR^TR+\sum_{k=1}^{g}\tau_k^2P^2(\xi^{-1}+n^{-1}+ga^{-1})\Big]E(t)\\
&+E^T(t)E(t)\\
&+\sum_{k=1}^{g}\sum_{i=1}^{u}h_i(t)E^T(t-\tau_k)\Big[ga\bar{A}_{ik}^T\bar{A}_{ik}\\
&-\psi_k]E(t-\tau_k)+\xi gD^T(t)D(t)-\rho^2D^T(t)D(t)\\
=&\sum_{i=1}^{u}\sum_{\ell=1}^{m}h_i(t)E^T(t)\Big[b(A_i-Z_\ell C)^T(A_i-Z_\ell C)\\
&+b^{-1}\sum_{k=1}^{g}\tau_k^2P^2+\sum_{k=1}^{g}\psi_k+I\\
&+ngR^TR+\sum_{k=1}^{g}\tau_k^2P^2(\xi^{-1}+n^{-1}+ga^{-1})\Big]E(t)\\
&+\sum_{k=1}^{g}\sum_{i=1}^{u}h_i(t)E^T(t-\tau_k)\Big[ga\bar{A}_{ik}^T\bar{A}_{ik}-\psi_k\Big]E(t-\tau_k)\\
&+(\xi g-\rho^2)D^T(t)D(t)\\
=&\sum_{i=1}^{u}\sum_{\ell=1}^{m}h_i(t)E^T(t)\Delta_{i\ell}E(t)\\
&+\sum_{i=1}^{u}\sum_{k=1}^{g}h_i(t)E^T(t-\tau_k)\nabla_{ik}E(t-\tau_k)+(\xi g-\rho^2)D^T(t)D(t)\\
&+(\xi g-\rho^2)D^T(t)D(t)<0 \qquad (3.11)
\end{aligned}
$$

where

$$
\begin{aligned}
\Delta_{i\ell}\ &\equiv b(A_i-Z_\ell C)^T(A_i-Z_\ell C)+\sum_{k=1}^{g}\psi_k+ngR^TR\\
&\quad+I+\sum_{k=1}^{g}\tau_k^2P^2(b^{-1}+\xi^{-1}+n^{-1}+ga^{-1})
\end{aligned}
$$

(see(3.5a))

$$\nabla_{ik}\equiv ga\bar{A}_{ik}^T\bar{A}_{ik}-\psi_k. \qquad \text{(see(3.5b))}$$

The following inequality can be obtained by integrating Eq. (3.11) from $t=0$ to $t=\infty$:

$$V(\infty)-V(0)+\int_0^\infty E^T(t)E(t)dt-\rho^2\int_0^\infty D^T(t)D(t)dt\leq 0.$$

Setting the initial conditions to be zero (i.e., $E(t)\equiv 0$ for $t\in[-\tau_{\max},0]$):

$$\int_0^\infty E^T(t)E(t)dt\leq\rho^2\int_0^\infty D^T(t)D(t)dt.$$

Thus, Eq. (3.4) and the H^∞ control performance is realized with a prescribed attenuation ρ.

The following inequality can be obtained from (3.11):

$$
\begin{aligned}
&\dot{V}(t)+E^T(t)E(t)-\rho^2D^T(t)D(t)\\
&<\sum_{i=1}^{u}\sum_{\ell=1}^{m}h_i(t)\left[\frac{\lambda_{\max}(\Delta_{i\ell})}{\sum_{k=1}^{g}\tau_k\lambda_{\min}(P)}\right]<0. \qquad (3.12)
\end{aligned}
$$

Then, the following is obtained:

$$V(t)\big|_{D(t)=0}\leq V(t_0)exp\bar{\beta}(t-t_0) \qquad (3.13)$$

where

$$\bar{\beta}=\sum_{i=1}^{u}\sum_{\ell=1}^{m}h_i(t)\left[\frac{\lambda_{\max}(\Delta_{i\ell})}{\sum_{k=1}^{g}\tau_k\lambda_{\min}(P)}\right].$$

Eqs. (3.6) and (3.13) show that:

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

That is,

$$\|E(t)\|^2<\frac{V(t_0)}{\sum_{k=1}^{g}\tau_k\lambda_{\min}(P)}exp\bar{\beta}(t-t_0).$$

Accordingly, it is concluded that:

$$\|E(t)\|\leq\alpha exp(-\beta(t-t_0))$$

with

$$\alpha\equiv\sqrt{\frac{V(t_0)}{\sum_{k=1}^{g}\tau_k\lambda_{\min}(P)}}>0\quad\text{and}\quad\beta\equiv-\frac{1}{2}\bar{\beta}>0.$$

Therefore, based on Definition 1, the error system (3.1) under the fuzzy observer (2.10) is exponentially stable for $D(t)=0$.

Corollary 1: We can reformulate Eqs. (3.5a) and (3.5b) into LMIs using the following procedure:

The new variables are introduced: $Q=P^{-1},\bar{\psi}_k=Q\psi_kQ^T$ and $F_l=Z_\ell Q$. Moreover, on the basis of Schur's complement [50], it is easy to show that the inequalities in Eqs. (3.5a) and (3.5b) are equivalent to the following LMIs in Eqs. (3.14a) and (3.14b):

$$\begin{bmatrix}\Xi & QR^T & (A_i-Z_\ell C)Q^T\\ RQ^T & -(ng)^{-1}I & 0\\ Q(A_i-Z_\ell C)^T & 0 & -(b^{-1})I\end{bmatrix}<0 \qquad (3.14a)$$

$$\begin{bmatrix}-\bar{\psi}_k & Q\bar{A}_{ik}^T\\ \bar{A}_{ik}Q & -(ga)^{-1}I\end{bmatrix}<0 \qquad (3.14b)$$

where

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

Accordingly, we can transform Theorem 1 into an LMI problem. Efficient interior-point algorithms are now obtainable in the Matlab LMI Solver to solve this problem.

Corollary 2 [51]: To certify whether solving the inequalities in Eqs. (3.14a) and (3.14b) by Matlab LMI Solver is feasible, we use interior-point optimization techniques to compute feasible solutions. These techniques need that the LMI systems are strictly feasible with a nonempty interior. For feasibility problems, the LMI Solver by the *feasp* is shown as follows:

$$\text{Find } x \text{ such that the LMI L(x)} < 0 \tag{3.15a}$$

as

$$\text{Minimize } t \text{ subject to L(x)} < t \times I \tag{3.15b}$$

where I denotes an identity matrix and L(x) denotes a symmetric matrix.

Based on Corollary 2, the LMI constraint is always strictly feasible in x, t, and the original LMI (3.15a) is feasible if and only if the global minimum $t$min of (3.15b) meets $t\text{min} < 0$. Namely, if $t\text{min} < 0$ meets Eqs. (3.14a) and (3.14b), then the stability conditions (3.5a) and (3.5b) in Theorem 1 can be satisfied. The error system can then be exponentially stabilized by the fuzzy observer (2.10), and the H^∞ control performance is simultaneously achieved.

Corollary 3: To accomplish exponential optimal H^∞ synchronization, the following constrained optimization problem formulates the fuzzy observer design:

$$\text{minimize } \rho > \sqrt{\xi g} \tag{3.16}$$

subject to $\bar{\psi}_k = \bar{\psi}_k^T > 0$, $Q = Q^T > 0$, (3.14a) and (3.14b).

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

IV. ALGORITHM

The complete design procedure can be summarized as follows.

Problem: Considering two multiple time-delay chaotic (MTDC) systems with different initial conditions and 3DES encryption/decryption schemes, the problem is focused on designing a fuzzy observer to accomplish exponential optimal H^∞ synchronization and to carry out double encryption by means of 3DES and chaotic synchronization.

On the basis of the illustration of Fig. 1 (which is shown in Section II), this problem could be solved through several steps. To make the encryption steps more comprehensible, the encryption process is divided into 9 steps as follows:

Step 1: The T-S fuzzy models of the master system (2.8) and the slave system (2.9) are constructed, respectively.

Step 2: The encrypted message (ciphertext) is got by three keys and the plaintext via the 3DES encryption function.

Step 3: The ciphertext is dispatched to the master system and transformed into the encrypted signal by chaotic masking. The encrypted signal is then forwarded to the slave system via the public channel.

Step 4: Based on the observer scheme, the gains of the model-based fuzzy observer (2.10) can be synthesized to exponentially stabilize the error system by the Matlab LMI Toolbox.

Step 5: According to the IGA process shown in subsection 2.4, the better observer gains are obtained to stabilize the MTDC systems.

Step 6: The synchronization error is then defined as: $E(t) = \hat{X}(t) - X(t)$, and we can get the dynamics of the error system (3.1).

Step 7: On the basis of Corollary 3, the positive constant ξ is minimized by the mincx function of the Matlab LMI Toolbox. The minimum disturbance attenuation level is then obtained.

Step 8: We can get matrices Q, F_l, and $\bar{\psi}_k$ with the minimum disturbance attenuation $\rho_{\min}$.

Step 9: The encrypted signal (chaotic masking signal) is filtered to get the ciphertext. Finally, the ciphertext is decrypted by three keys and it is converted into the plaintext by means of the 3DES decryption function.

V. NUMERICAL EXAMPLE

The following example demonstrates the effectiveness of the aforementioned algorithm.

Problem: This example aims to design a fuzzy observer to realize optimal H^∞ exponential synchronization, to combine the concepts of chaotic synchronization, and the cryptography of the 3DES algorithm to get a more secure communication chaotic synchronization cryptosystem. Consider a pair of modified multiple time-delay Liu's chaotic systems in a master-slave configuration, as depicted below:

$$\begin{cases} \dot{x}_1(t) = 0.5\,(x_2(t) - x_1(t)) \\ \dot{x}_2(t) = -7.5x_1(t) - 0.15x_1(t)x_3(t) \\ \dot{x}_3(t) = -5.5x_3(t) + 2x_1^2(t) + 0.4x_1(t-0.15) \\ +0.4x_2(t-0.09) + 0.4x_3(t-0.08) \end{cases} \tag{5.1}$$

and

$$\begin{cases} \dot{\hat{x}}_1(t) = 0.5\left(\hat{x}_2(t) - \hat{x}_1(t)\right) + d(t) \\ \dot{\hat{x}}_2(t) = -7.5\hat{x}_1(t) - 0.15\hat{x}_1(t)\hat{x}_3(t) + d(t) \\ \dot{\hat{x}}_3(t) = -5.5\hat{x}_3(t) + 2\hat{x}_1^2 + 0.4\hat{x}_1(t-0.15) \\ \qquad\qquad +0.4\hat{x}_2(t-0.09) + 0.4\hat{x}_3(t-0.08) + d(t) \end{cases} \tag{5.2}$$

in which $\left[\,x_1(t)\ x_2(t)\ x_3(t)\,\right]^T$ is the state vector of the master system and $\left[\,x_1(t)\ x_2(t)\ x_3(t)\,\right]^T$ denotes the state vector of the slave system. Setting the initial conditions of master and slave systems as:

$[x_1(0) = 1.55,\ x_2(0) = -1.66,\ x_3(0) = 1.38]$ and

$[\hat{x}_1(0) = 0.95\ \hat{x}_2(0) = -1.3\ \hat{x}_3(0) = 1.2]$, and let the external disturbance $d(t)$ be:

$$d(t) = 0.2\sin(2t),\ 0 \le \mathrm{t} \le 6 \tag{5.3}$$

Solution: The solution to the above problem is described as:

Step 1: The T-S fuzzy models are constructed for the master and slave systems, respectively. To minimize the design effort and complexity, this study uses as few rules as possible. The chaotic systems (5.1-5.2) are therefore approximated with the following fuzzy models:

A. THE FUZZY MODEL OF THE MASTER SYSTEM

Rule 1: IF $x_1(t)$ is M_{11},
THEN

$$\begin{aligned}\dot{X}(t) &= A_1X(t) + \sum_{k=1}^{3}\bar{A}_{1k}X(t-\tau_k),\\ Y(t) &= CX(t)\end{aligned} \tag{5.4a}$$

Rule 2: IF $x_1(t)$ is M_{21},
THEN

$$\begin{aligned}\dot{X}(t) &= A_2X(t) + \sum_{k=1}^{3}\bar{A}_{2k}X(t-\tau_k),\\ Y(t) &= CX(t)\end{aligned} \tag{5.4b}$$

where $X(t) = [x_1(t)x_2(t)x_3(t)]^T$, $\tau_1 = 0.15$, $\tau_2 = 0.09$, $\tau_3 = 0.08$

$$A_1 = \begin{bmatrix} -0.5 & 0.5 & 1\\ -7.5 & 0 & 0\\ 3.55 & 0 & -5.5 \end{bmatrix},\ A_2 = \begin{bmatrix} -0.5 & 0.5 & 1\\ -7.5 & 0 & 0\\ 0.593 & 0 & -5.5 \end{bmatrix},$$

$$\bar{A}_{11} = \begin{bmatrix} 0 & 0 & 0\\ 0 & 0 & 0\\ 0.4 & 0 & 0 \end{bmatrix},\ \bar{A}_{21} = \begin{bmatrix} 0 & 0 & 0\\ 0 & 0 & 0\\ 0.4 & 0 & 0 \end{bmatrix},$$

$$\bar{A}_{12} = \begin{bmatrix} 0 & 0 & 0\\ 0 & 0 & 0\\ 0 & 0.4 & 0 \end{bmatrix},\ \bar{A}_{22} = \begin{bmatrix} 0 & 0 & 0\\ 0 & 0 & 0\\ 0 & 0.4 & 0 \end{bmatrix},$$

$$\bar{A}_{13} = \begin{bmatrix} 0 & 0 & 0.4\\ 0 & 0 & 0\\ 0 & 0 & 0 \end{bmatrix},\ \bar{A}_{23} = \begin{bmatrix} 0 & 0 & 0.4\\ 0 & 0 & 0\\ 0 & 0 & 0 \end{bmatrix}. \tag{5.5}$$

and the membership functions for Rule 1 and Rule 2 are:

$$M_{11}(x_1(t)) = \begin{cases} 1, & x_1(t) > 3.5\\ \dfrac{x_1(t) - 0.593}{3.5 - 0.593}, & 3.5 > x_1(t) > 0.593\\ 0, & x_1(t) < 0.593 \end{cases} \tag{5.6a}$$

$$M_{21}(x_1(t)) = 1 - M_{11}(x_1(t)). \tag{5.6b}$$

B. THE FUZZY MODEL OF THE SLAVE SYSTEM IS

Rule 1: IF $\hat{x}_1(t)$ is $\hat{M}_{11}$,
THEN

$$\begin{aligned}\dot{\hat{X}}(t) &= \hat{A}_1\hat{X}(t) + \sum_{k=1}^{3}\hat{\bar{A}}_{1k}\hat{X}(t-\tau_k) + D(t)\\ \hat{Y}(t) &= C\hat{X}(t)\end{aligned} \tag{5.7a}$$

Rule 2: IF $\hat{x}_1(t)$ is $\hat{M}_{21}$,
THEN

$$\begin{aligned}\dot{\hat{X}}(t) &= \hat{A}_2\hat{X}(t) + \sum_{k=1}^{3}\hat{\bar{A}}_{2k}\hat{X}(t-\tau_k) + D(t),\\ \hat{Y}(t) &= C\hat{X}(t)\end{aligned} \tag{5.7b}$$

where $\left[\, x_1(t)\ x_2(t)\ x_3(t) \,\right]^T$, $\tau_1 = 0.15$, $\tau_2 = 0.09$, $\tau_3 = 0.08$.

$$\hat{A}_1 = \begin{bmatrix} -0.5 & 0.5 & 1\\ -7.5 & 0 & 0\\ 2.9503 & 0 & -5.5 \end{bmatrix}\ \hat{A}_2 = \begin{bmatrix} -0.5 & 0.5 & 1\\ -7.5 & 0 & 0\\ 1.11 & 0 & -5.5 \end{bmatrix},$$

$$\hat{\bar{A}}_{11} = \begin{bmatrix} 0 & 0 & 0\\ 0 & 0 & 0\\ 0.4 & 0 & 0 \end{bmatrix},\ \hat{\bar{A}}_{21} = \begin{bmatrix} 0 & 0 & 0\\ 0 & 0 & 0\\ 0.4 & 0 & 0 \end{bmatrix},$$

$$\hat{\bar{A}}_{12} = \begin{bmatrix} 0 & 0 & 0\\ 0 & 0 & 0\\ 0 & 0.4 & 0 \end{bmatrix},\ \hat{\bar{A}}_{22} = \begin{bmatrix} 0 & 0 & 0\\ 0 & 0 & 0\\ 0 & 0.4 & 0 \end{bmatrix},$$

$$\hat{\bar{A}}_{13} = \begin{bmatrix} 0 & 0 & 0\\ 0 & 0 & 0\\ 0 & 0 & 0.4 \end{bmatrix},\ \hat{\bar{A}}_{23} = \begin{bmatrix} 0 & 0 & 0\\ 0 & 0 & 0\\ 0 & 0 & 0.4 \end{bmatrix}. \tag{5.8}$$

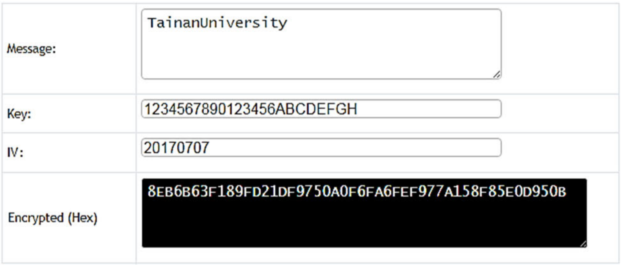
and the membership functions for Rules 1 and 2 are:

$$\hat{M}_{11}(\hat{x}_1(t)) = \begin{cases} 1, & \hat{x}_1(t) > 2.9503\\ \dfrac{\hat{x}_1(t) - 1.11}{2.9503 - 1.11}, & 2.9503 > \hat{x}_1(t) > 1.11\\ 0, & \hat{x}_1(t) < 1.11 \end{cases} \tag{5.9a}$$

$$\hat{M}_{21}(\hat{x}_1(t)) = 1 - \hat{M}_{11}(\hat{x}_1(t)). \tag{5.9b}$$

Step 2: Assuming the plaintext is "Tainan University". Set key as "1234567890123456ABCDEFGH". Set initialization vector: 20170707.

Then, the 3DES algorithm can be started in CBC mode which is shown in subsection 2.1 (Fig. 5). The plaintext is then encrypted as below (Fig. 6):



Message:	TainanUniversity
Key:	1234567890123456ABCDEFGH
IV:	20170707
Encrypted (Hex)	8EB6B63F189FD21DF9750A0F6FA6FEF977A158F85E0D950B

FIGURE 6. The encrypted message.

The encrypted message (ciphertext) is obtained as follows: "8EB6B63F189FD21DF9750A0F6FA6FEF977A158F85E0D950B"

To deliver the encrypted message to the master system, it is converted into decimal as follows:

"349933019212411854599579773778528429733440911 3357823874315"

The value is too large, therefore, it is multiplied by 10^{-58}, and the encrypted message (ciphertext)$\boldsymbol{\imath}(\cdot)$ is obtained as follows:

"0.349933019212411854599579773778528429733440911 3357823874315"

Step 3: The encrypted message $\boldsymbol{\imath}(\cdot)$ is then dispatched to the master system (5.1), which is converted into the encrypted signal by chaotic masking. The encrypted signal shown in (5.10) is then forwarded to the slave system via the public channel.

$$X(t):\begin{cases}\dot{x}_1(t)=0.5(x_2(t)-x_1(t))+\boldsymbol{\imath}(\cdot)\\ \dot{x}_2(t)=-7.5x_1(t)-0.15x_1(t)x_3(t)\\ \dot{x}_3(t)=-5.5x_3(t)+2x_1^2(t)+0.4x_1(t-0.15)\\ \qquad\qquad +0.4x_2(t-0.09)+0.4x_3(t-0.08).\end{cases} \tag{5.10}$$

Step 4: To synchronize the master and slave systems, a fuzzy observer is synthesized as:

Observer Rule 1: IF $\hat{x}_1(t)$ is $\bar{M}_{11}$,
THEN

$$\dot{\hat{X}}(t)=A_1\hat{X}(t)+\sum_{k=1}^{3}\hat{\bar{A}}_{1k}\hat{X}(t-\tau_k)+D(t)+Z_1(Y(t)-\hat{Y}(t)),$$
$$\hat{Y}(t)=C\hat{X}(t). \tag{5.11a}$$

Observer Rule 2: IF $\hat{x}_1(t)$ is $\bar{M}_{21}$,
THEN

$$\dot{\hat{X}}(t)=A_2\hat{X}(t)+\sum_{k=1}^{3}\hat{\bar{A}}_{2k}\hat{X}(t-\tau_k)+D(t)+Z_2(Y(t)-\hat{Y}(t)),$$
$$\hat{Y}(t)=C\hat{X}(t). \tag{5.11b}$$

$\bar{M}_{11}$ and $\bar{M}_{21}$ are the membership functions for each $\hat{x}_1$ (see Fig. 7):

$$\bar{M}_{11}(\hat{x}_1(t))=\frac{1}{2}(1+\frac{\hat{x}_1(t)}{30}) \tag{5.12a}$$
$$\bar{M}_{21}(\hat{x}_1(t))=\frac{1}{2}(1-\frac{\hat{x}_1(t)}{30}) \tag{5.12b}$$

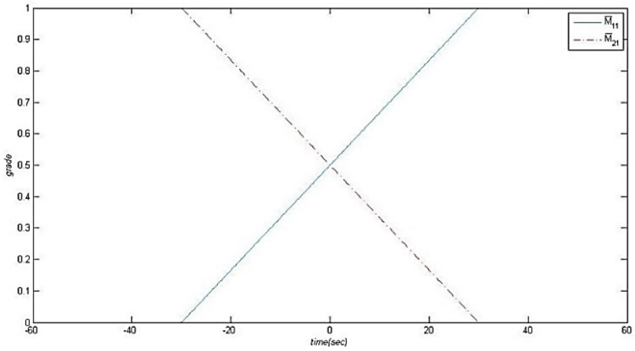


FIGURE 7. Membership functions of the fuzzy observer.

Based on Eq. (3.1), the dynamics of the error system is obtained as:

$$\dot{E}(t)=\sum_{i=1}^{2}\sum_{k=1}^{3}\sum_{\ell}^{2}h_i(t)\left\{(A_i-Z_\ell C)E(t)+\bar{A}_{ik}E(t-\tau_k)\right\}$$
$$+D(t)+\Phi(t) \tag{5.13}$$

where

$$\hat{\Psi}\equiv f(\hat{X}(t))+\sum_{k=1}^{3}H_k(\hat{X}(t-\tau_k))+Z_\ell(Y(t)-\hat{Y}(t)),$$
$$\Psi\equiv f(X(t))+\sum_{k=1}^{3}H_k(X(t-\tau_k))+\boldsymbol{\imath}(\cdot)$$

with

$$\Phi(t)\equiv\hat{\psi}-\psi$$
$$-\left\{\sum_{i=1}^{2}\sum_{k=1}^{3}\sum_{\ell=1}^{2}h_i(t)\left[(A_i-Z_\ell C)E(t)+\bar{A}_{ik}E(t-\tau_k)\right]\right\}.$$

Step 5: Based on the LMI approach and the IGA process to obtain better observer gains. In this study, two demonstrations of the performance of the observer gains are examined.

C. METHOD 1 (LMI)

Based on Eqs. (5.4a-5.9b and 5.11a-5.13), the LMIs in Eqs. (3.14a) and (3.14b) can be solved using the Matlab LMI Toolbox with $a=b=\xi=n=1$, and the resulting observer gains are:

$$Z_1=\begin{bmatrix}1244.4304 & -0.0009210 & 0.0005999\\ -0.0009295 & 1244.4305 & 0.0000011\\ 0.0006029 & -0.0000011 & 1244.4291\end{bmatrix}, \tag{5.14a}$$

$$Z_2=\begin{bmatrix}1244.4302 & -0.0009214 & 0.0002026\\ -0.0009292 & 1244.4304 & -0.0000005\\ 0.0002044 & 0.0000005 & 1244.4289\end{bmatrix}. \tag{5.14b}$$

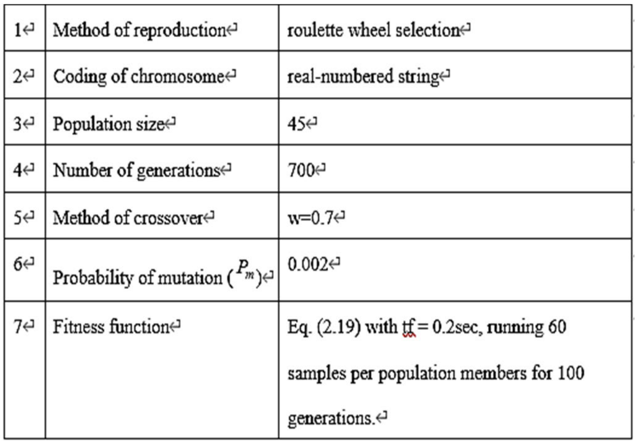
D. METHOD 2 (IGA(LMI))

IGA has the ability of random search for near-optimal solutions, therefore, it can search better fuzzy observer gains to speed up the synchronization. Based on the observer gains obtained by the Matlab LMI toolbox in Eqs. (5.14a-5.14b), the lower and upper bounds of the search space are set as (Z_{1d}, Z_{2d})[1] $\in [1200, 1600]$ and (Z_{1c}, Z_{2c})[2] $\in [-10, 10]$ for $d = 1, 5, 9$; $c = 2, 3, 4, 6, 7, 8$. Prior to carrying out the searching process using the IGA, some specifications are shown in Table 8.

[1] The representations of (Z_{1d}, Z_{2d}) and (Z_{1c}, Z_{2c}) for $d = 1, 5, 9$ (diagonal); $c = 2, 3, 4, 6, 7, 8$ (off-diagonal) are described as $Z_1 = \begin{bmatrix}Z_{11} & Z_{12} & Z_{13}\\ Z_{14} & Z_{15} & Z_{16}\\ Z_{17} & Z_{18} & Z_{19}\end{bmatrix}$ and$Z_2 = \begin{bmatrix}Z_{21} & Z_{22} & Z_{23}\\ Z_{24} & Z_{25} & Z_{26}\\ Z_{27} & Z_{28} & Z_{29}\end{bmatrix}$.

[2] To decrease the computational burden, this research sets the off-diagonal as small as possible (the off-diagonal approaches zero). Finding the diagonal matrices can possibly simplify our calculations and make them less time consuming.

TABLE 8. Specifications for IGA.



1↵	Method of reproduction↵	roulette wheel selection↵
2↵	Coding of chromosome↵	real-numbered string↵
3↵	Population size↵	45↵
4↵	Number of generations↵	700↵
5↵	Method of crossover↵	w=0.7↵
6↵	Probability of mutation (P_m)↵	0.002↵
7↵	Fitness function↵	Eq. (2.19) with tf = 0.2sec, running 60 samples per population members for 100 generations.↵

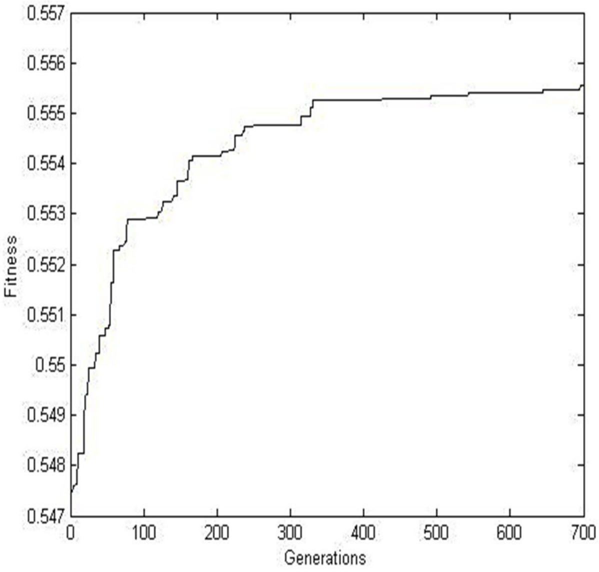


FIGURE 8. Fitness values of IGA.

After performing the IGA search process, the resulting observer gains are obtained and the fitness values of IGA is shown in Fig. 8:

$$Z_1 = \begin{bmatrix} 1597.6283 & -7.4836200 & 8.7621800 \\ 9.6944300 & 1400.9561 & 9.9014500 \\ 9.6277400 & -9.7508100 & 1599.7781 \end{bmatrix}, \quad (5.15a)$$

$$Z_2 = \begin{bmatrix} 1596.4355 & -4.3762700 & 4.4794000 \\ 9.1058800 & 1400.0444 & 1.0000000 \\ 9.6438700 & -9.0121800 & 1599.5235 \end{bmatrix}, \quad (5.15b)$$

Steps 6-7: According to Eqs. (5.4a-5.9b, 5.11a-5.15b), LMIs in Eqs. (3.14a) and (3.14b) can be solved using the Matlab LMI Toolbox. The specified structured bounding matrix R and ε_i can be set as: $R = \begin{bmatrix} 5000 & 0 & 0 \\ 0 & 5000 & 0 \\ 0 & 0 & 5000 \end{bmatrix}$, $\varepsilon_i = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$. On the basis of Corollary 3, the positive constant ξ is minimized by the mincx function of the Matlab LMI Toolbox: $\xi_{\min} = 1.463061 \times 10^{-6}$; the minimum disturbance attenuation level is $\rho_{\min} = 2.095 \times 10^{-3}$.

Step 8: The common solutions Q, F_1, F_2, $\bar{\psi}_1$, $\bar{\psi}_2$, and $\bar{\psi}_3$ of stability conditions (3.14a) and (3.14b) can be obtained with the best value *stmin* of the LMI Solver (Matlab), which is -1.293955×10^{-4}:

$$Q = 10^{-3} \times \begin{bmatrix} 0.2765 & 0.0001 & -0.0003 \\ 0.0001 & 0.2795 & 0.0002 \\ -0.0003 & 0.0002 & 0.2764 \end{bmatrix}, \quad (5.16)$$

$$F_1 = \begin{bmatrix} 0.4417 & -0.0019 & 0.0019 \\ 0.0028 & 0.3916 & 0.0030 \\ 0.0022 & -0.0024 & 0.4422 \end{bmatrix}, \quad (5.17a)$$

$$F_2 = \begin{bmatrix} 0.4414 & -0.0010 & 0.0007 \\ 0.0027 & 0.3913 & 0.0030 \\ 0.0022 & -0.0022 & 0.4421 \end{bmatrix}, \quad (5.17b)$$

$$\bar{\psi}_1 = \bar{\psi}_2 = \bar{\psi}_3 = 10^7 \times \begin{bmatrix} 5.1638 & 0.0115 & 0.0509 \\ 0.0115 & 4.2276 & 0.0035 \\ 0.0509 & 0.0035 & 5.1775 \end{bmatrix}, \quad (5.18)$$

Fig.9 demonstrates that the synchronization errors (e_1, e_2 and e_3) according to the IGA method have better convergent speed than those of the LMI approach. Fig. 10 shows the state responses of both the master and slave systems. Furthermore, the assumption $\|\Phi(t)\| \le \left\| \sum_{i=1}^{2} \sum_{l=1}^{2} h_i(t)\varepsilon_{il}^{qq} RE(t) \right\|$ is met from the illustration given in Fig. 11. In the end, the simulation results show that the exponential H^∞ synchronization of MTDC secure communication systems can retrieve the transmitted message using the designed fuzzy observer.

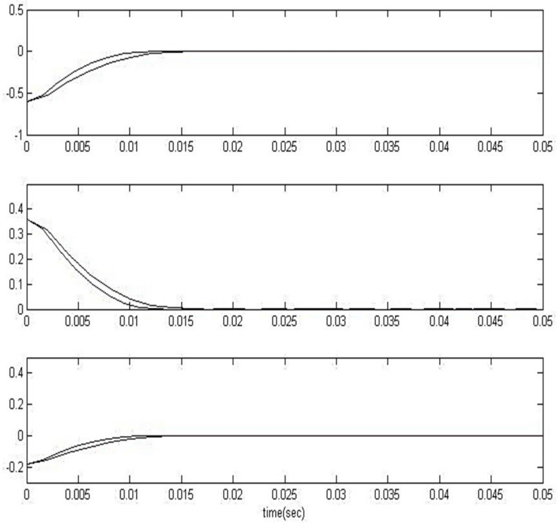


FIGURE 9. State responses of LMI $e_1e_2e_3$ (red line) and IGA $e_1e_2e_3$ (blue line).

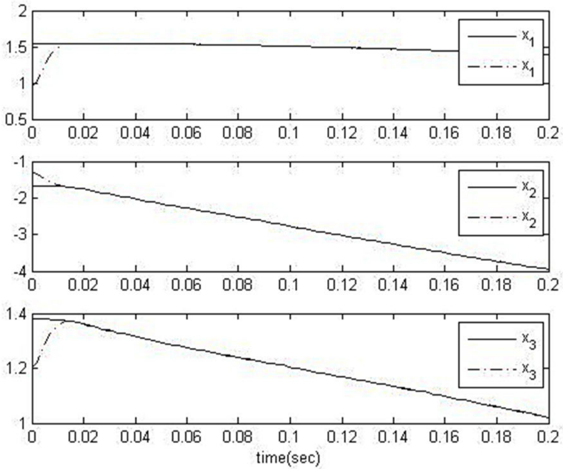


FIGURE 10. State responses of both master and slave systems.

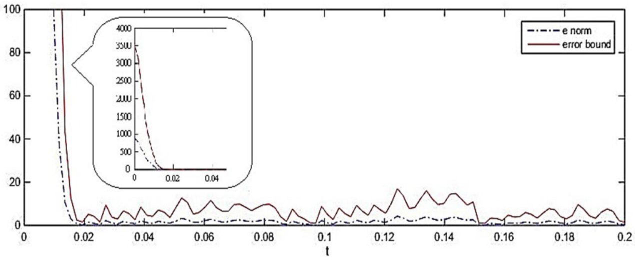


FIGURE 11. Plots of $\|\Phi(t)\|$ (blue line) and $\|\Phi(t)\| \leq \left\|\sum_{i=1}^{2}\sum_{l=1}^{2} h_i(t)\varepsilon_{il}^{qq}RE(t)\right\|$ (red line).

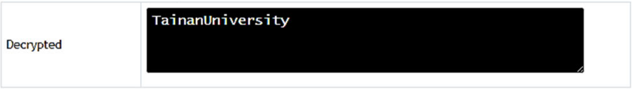

Decrypted
TainanUniversity

FIGURE 12. The decrypted message.

Step 9: When the master system is synchronized with the slave system, the plaintext can be restored from the decryption function. The encrypted message $\iota(\cdot)$ is thus obtained as:

"0.34993301921241185459957977377852842973344091133578238743 15"

After obtaining the encrypted message, it is multiplied by 10^{58}:

"349933019212411854599579773778528429733440911335782387431 5"

The encrypted message m is then converted to the Hex code:

"8EB6B63F189FD21DF9750A0F6FA6FEF977A158F85E0D950B"

The 3DES algorithm can then be started in the CBC mode to decrypt the encrypted message, where the decryption procedure of 3DES can be performed in the same way as the encryption procedure by reversing the order of the subkeys, which is one of the merits of Feistel networks.

Finally, the plaintext is obtained (Fig. 12):

"Tainan University"

VI. CONCLUSION

In this study, we propose a novel approach to achieve the exponential optimal H^∞ synchronization of MTDC systems. To prohibit hackers from stealing personal information, the concept of double encryption is applied to combine chaotic synchronization with the 3DES algorithm to enhance the complexity of the cryptosystem. The proposed method not only establishes a more secure communication system but adequately protects the ciphertext as well.

REFERENCES

[1] Y. Sheng, H. Zhang, and Z. Zeng, "Stabilization of fuzzy memristive neural networks with mixed time delays," *IEEE Trans. Fuzzy Syst.*, vol. 26, no. 5, pp. 2591–2606, Oct. 2018.

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

[3] C. Hu, H. Jiang, and Z. Teng, "General impulsive control of chaotic systems based on a TS fuzzy model," *Fuzzy Sets Syst.*, vol. 174, no. 1, pp. 66–82, Jul. 2011.

[4] A. Jimenez-Triana, W. Kit-Sang Tang, G. Chen, and A. Gauthier, "Chaos control in duffing system using impulsive parametric perturbations," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 57, no. 4, pp. 305–309, Apr. 2010.

[5] J. Ahmad, A. Tahir, J. S. Khan, A. Jameel, Q. H. Abbasi, and W. Buchanan, "A novel multi-chaos based compressive sensing encryption technique," in *Proc. Int. Conf. Adv. Emerg. Comput. Technol. (AECT)*, Feb. 2020, pp. 1–4.

[6] 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.

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

[8] H. K. Lam, W. K. Ling, H. H. Iu, and S. S. Ling, "Synchronization of chaotic systems using time-delayed fuzzy state-feedback controller," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 55, no. 3, pp. 893–903, May 2008.

[9] A. Loria and A. Zavala-Rio, "Adaptive tracking control of chaotic systems with applications to synchronization," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 54, no. 9, pp. 2019–2029, Sep. 2007.

[10] H. Dimassi and A. Loria, "Adaptive unknown-input observers-based synchronization of chaotic systems for telecommunication," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 58, no. 4, pp. 800–812, Apr. 2011.

[11] T. Wang, D. Wang, and K. Wu, "Chaotic adaptive synchronization control and application in chaotic secure communication for industrial Internet of Things," *IEEE Access*, vol. 6, pp. 8584–8590, 2018.

[12] A. Mohammadzadeh, O. Kaynak, and M. Teshnehlab, "Two-mode indirect adaptive control approach for the synchronization of uncertain chaotic systems by the use of a hierarchical interval type-2 fuzzy neural network," *IEEE Trans. Fuzzy Syst.*, vol. 22, no. 5, pp. 1301–1312, Oct. 2014.

[13] T.-C. Lin and T.-Y. Lee, "Chaos synchronization of uncertain fractional-order chaotic systems with time delay based on adaptive fuzzy sliding mode control," *IEEE Trans. Fuzzy Syst.*, vol. 19, no. 4, pp. 623–635, Aug. 2011.

[14] S. Wen, T. Huang, X. Yu, Z. Q. M. Chen, and Z. Zeng, "Aperiodic sampled-data sliding-mode control of fuzzy systems with communication delays via the event-triggered method," *IEEE Trans. Fuzzy Syst.*, vol. 24, no. 5, pp. 1048–1057, Oct. 2016.

[15] W. Wang, P. H. A. J. M. Van Gelder, and J. K. Vrijling, "The effects of dynamical noises on the identification of chaotic systems: With application to streamflow processes," in *Proc. 4th Int. Conf. Natural Comput.*, Jinan, China, Oct. 2008, pp. 685–691.

[16] Y. Xia, Z. Yang, and M. Han, "Lag synchronization of unknown chaotic delayed Yang–Yang-type fuzzy neural networks with noise perturbation based on adaptive control and parameter identification," *IEEE Trans. Neural Netw.*, vol. 20, no. 7, pp. 1165–1180, Jul. 2009.

[17] Y.-Y. Hou, T.-L. Liao, and J.-J. Yan, "H_∞ synchronization of chaotic systems using output feedback control design," *Phys. A, Stat. Mech. Appl.*, vol. 379, no. 1, pp. 81–89, 2007.

[18] C. K. Ahn, P. Shi, and L. Wu, "Receding horizon stabilization and disturbance attenuation for neural networks with time-varying delay," *IEEE Trans. Cybern.*, vol. 45, no. 12, pp. 2680–2692, Dec. 2015.

[19] C. K. Ahn, S. Han, and W. H. Kwon, "H_∞ finite memory controls for linear discrete-time state-space models," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 54, no. 2, pp. 97–101, Feb. 2007.

[20] U. Parlitz, L. Kocarev, and H. G. Schuster, *Handbook of Chaos Control*. Hoboken, NJ, USA: Wiley, 1999.

[21] C. K. Ahn, S. T. Jung, S. K. Kang, and S. C. Joo, "Adaptive H_∞ synchronization for uncertain chaotic systems with external disturbance," *Commun. Nonlinear Sci. Numer. Simul.*, vol. 15, no. 8, pp. 2168–2177, 2010.

[22] H. R. Karimi and H. Gao, "New delay-dependent exponential H_∞ synchronization for uncertain neural networks with mixed time delays," *IEEE Trans. Syst., Man, Cybern. B, Cybern.*, vol. 40, no. 1, pp. 173–185, Feb. 2010.

[23] H. R. Karimi and P. Maass, "Delay-range-dependent exponential H_∞ synchronization of a class of delayed neural networks," *Chaos, Solitons Fractals*, vol. 41, no. 3, pp. 1125–1135, Aug. 2009.

[24] Z. Zhao, F. Lv, J. Zhang, and Y. Du, "H_∞ synchronization for uncertain time-delay chaotic systems with one-sided Lipschitz nonlinearity," *IEEE Access*, vol. 6, pp. 19798–19806, 2018.

[25] S. H. Ling and F. H. F. Leung, "An improved genetic algorithm with average-bound crossover and wavelet mutation operations," *Soft Comput.*, vol. 11, no. 1, pp. 7–31, Jan. 2007.

[26] C. C. Cheng and C. C. Wong, "Self-generating rule-mapping fuzzy controller design using a genetic algorithm," *IEE Proc., Control Theory Appl.*, vol. 149, no. 2, pp. 143–148, 2002.

[27] S. H. Ling, F. H. F. Leung, H. K. Lam, Y.-S. Lee, and P. K. S. Tam, "A novel genetic-algorithm-based neural network for short-term load forecasting," *IEEE Trans. Ind. Electron.*, vol. 50, no. 4, pp. 793–799, Aug. 2003.

[28] K. F. Leung, F. H. F. Leung, H. K. Lam, and S. H. Ling, "On interpretation of graffiti digits and characters for eBooks: Neural-fuzzy network and genetic algorithm approach," *IEEE Trans. Ind. Electron.*, vol. 51, no. 2, pp. 464–471, Apr. 2004.

[29] S.-C. Huang, M.-K. Jiau, and C.-H. Lin, "Optimization of the carpool service problem via a fuzzy-controlled genetic algorithm," *IEEE Trans. Fuzzy Syst.*, vol. 23, no. 5, pp. 1698–1712, Oct. 2015.

[30] 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.

[31] C.-L. Chiang, "Improved genetic algorithm for power economic dispatch of units with valve-point effects and multiple fuels," *IEEE Trans. Power Syst.*, vol. 20, no. 4, pp. 1690–1699, Nov. 2005.

[32] J. Zhang, Y. Shang, R. Gao, and Y. Dong, "An improved genetic algorithm based on J_1 triangulation and fixed point theory," in *Proc. 2nd IEEE Int. Conf. Comput. Sci. Inf. Technol.*, Beijing, China, Aug. 2009, pp. 138–142.

[33] J. Sun, F. Zhao, and L. Zhang, "An improved genetic algorithm for the multi-echelon inventory problem of repairable spare parts," *IEEE Trans. Intell. Comput. Intell. Syst.*, vol. 1, pp. 440–444, Oct. 2010. [Online]. Available: https://ieeexplore.ieee.org/document/5658605

[34] D. Coppersmith, D. B. Johnson, and S. M. Matyas, "A proposed mode for triple-DES encryption," *IBM J. Res. Develop.*, vol. 40, no. 2, pp. 253–262, Mar. 1996.

[35] C. J. Mitchell, "On the security of 2-key triple DES," *IEEE Trans. Inf. Theory*, vol. 62, no. 11, pp. 6260–6267, Nov. 2016.

[36] Y. Jun, L. Na, and D. Jun, "A design and implementation of high-speed 3DES algorithm system," in *Proc. 2nd Int. Conf. Future Inf. Technol. Manage. Eng.*, Sanya, China, Dec. 2009, pp. 175–178.

[37] Z. Yingbing and L. Yongzhen, "The design and implementation of a symmetric encryption algorithm based on DES," in *Proc. IEEE 5th Int. Conf. Softw. Eng. Service Sci.*, Beijing, China, Jun. 2014, pp. 517–520.

[38] Y. Ren, L. Wu, H. Li, X. Li, X. Zhang, A. Wang, and H. Chen, "Key recovery against 3DES in CPU smart card based on improved correlation power analysis," *Tsinghua Sci. Technol.*, vol. 21, no. 2, pp. 210–220, Apr. 2016.

[39] V. M. Silva-García, R. F. Carapia, I. López-Yáñez, and C. Rentería-Márquez, "Image encryption based on the modified triple-DES cryptosystem," *Int. Math. Forum*, vol. 7, no. 59, pp. 2929–2942, 2012.

[40] V. M. Silva-Garcia, R. Flores-Carapia, and C. Renteria-Marquez, "Triple-DES block of 96 bits: An application to colour image encryption," *Appl. Math. Sci.*, vol. 7, pp. 1143–1155, 2013.

[41] H. Handschuh and B. Prenee, "On the security of double and 2-key triple modes of operation," in *Fast Software Encryption* (Lecture Notes in Computer Science), vol. 1636. Berlin, Germany: Springer, 1999, pp. 215–230. [Online]. Available: https://link.springer.com/chapter/10.1007%2F3-540-48519-8_16#citeas

[42] T. Schaffer, A. Glaser, and P. D. Franzon, "Chip-package co-implementation of a triple DES processor," *IEEE Trans. Adv. Packag.*, vol. 27, no. 1, pp. 194–202, Feb. 2004.

[43] G. C. Cardarilli, L. Di Nunzio, R. Fazzolari, and M. Re, "TDES cryptography algorithm acceleration using a reconfigurable functional unit," in *Proc. 21st IEEE Int. Conf. Electron., Circuits Syst. (ICECS)*, Marseille, France, Dec. 2014, pp. 419–422.

[44] W. C. Barker and E. B. Barker, "Recommendation for the triple data encryption algorithm (TDEA) block cipher," NIST, Gaithersburg, MD, USA, Tech. Rep. NIST SP 800-67 Rev 1, 2012.

[45] 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./Feb. 1985.

[46] 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.

[47] 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, pp. 72–78, 1992.

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

[49] F. Hsiao, "An observer-based exponential synchronization scheme for chaotic systems: Using advanced encryption standard as auxiliary," *Asian J. Control*, vol. 22, no. 6, pp. 2183–2205, Nov. 2020.

[50] 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.

[51] P. Gahinet, A. Nemirovski, A. J. Laub, and M. Chilali, "LMI control toolbox user's guide," MathWorks, Natick, MA, USA, Tech. Rep., 1995. [Online]. Available: https://www.researchgate.net/publication/3611303_LMI_control_toolbox_user's_guide

FENG-HSIAG HSIAO was born in Tainan, Taiwan, in 1960. He received the Ph.D. degree in electrical engineering from the 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.