Received April 27, 2021, accepted May 12, 2021, date of publication May 17, 2021, date of current version May 28, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3080696

Synchronization of Chaotic System Using a Brain-Imitated Neural Network Controller and Its Applications for Secure Communications

CHIH-MIN LIN[1], (Fellow, IEEE), DUC-HUNG PHAM[1,2], AND TUAN-TU HUYNH[1,3], (Member, IEEE)

[1]Department of Electrical Engineering, Yuan Ze University, Taoyuan 320, Taiwan
[2]Faculty of Electrical and Electronic Engineering, Hung Yen University of Technology and Education, Hai Duong 160000, Vietnam
[3]Faculty of Mechatronics and Electronics, Lac Hong University, Bien Hoa 810000, Vietnam

Corresponding authors: Chih-Min Lin (cml@saturn.yzu.edu.tw) and Tuan-Tu Huynh (huynhtuantu@saturn.yzu.edu.tw)

This work was supported by the Ministry of Science and Technology of Republic of China under Grant MOST 109-2811-E-155-504-MY3.

ABSTRACT This paper proposes a new hybrid algorithm for secure communication applications. The proposed algorithm includes a fuzzy brain emotional learning controller (FBELC), a recurrent cerebellar model articulation controller (RCMAC), and a robust compensator (RC). The main brain-imitated neural network controller is a combination of the RCMAC and the FBELC, which is a mathematical model that approximates the decision and emotional activity of a human brain. A fuzzy inference system is also merged into the FBELC to produce an efficient hybrid structure, then it is used for secure communication applications. The 3-dimensional (3D) Genesio chaotic system is used for audio and image secure communication systems to show the potency and performance of the proposed algorithm. In the first application, a new image encryption algorithm is proposed to enhance security for information transmission, then several standard images are applied for the chaotic synchronization of image secure communication. In the second application, the audio signal is embedded in a 3D chaotic trajectory, which is used as an encryption carrier signal, after using the proposed method for the decryption, the source signal can be retrieved. The comparisons of simulation results using security analyses and root mean square error for recent algorithms are performed to validate the performance and efficiency of the proposed hybrid algorithm. The simulation results point out that our algorithm can attain better synchronization performance, and achieve more efficient audio and image secure communications.

INDEX TERMS Fuzzy inference system, brain emotional learning control, recurrent cerebellar model articulation controller, 3D chaotic systems, audio secure communication, image secure communication.

I. INTRODUCTION

Chaos is a remarkably fascinating phenomenon, which has been widely studying in the past decades [1]–[5]. It is sensitive to initial values, non-periodic, trajectory unpredictability, thus chaos theory is usually applied for secure communication [6], image encryption [7], signal processing [8], cryptography [9], etc. The synchronization of chaotic systems is one of the hot topics that attract many scholars over the years. Since the complete synchronization method of chaotic systems was introduced in 1990 [10], new methods and achievements are also increasingly efficient in chaotic synchronization. Particularly, Lin and Chung introduced a fuzzy brain emotion learning controller (BELC) with an effective computation and fast convergence. A fuzzy neural network (NN) combining with a BELC and a fuzzy inference rules was designed to synchronize a chaotic system [11]. A hybrid neural network including a fuzzy recurrent cerebellar model articulation controller (CMAC) network and a BELC network was proposed for chaotic synchronization [12]. An interval type-2 fuzzy BELC for three-dimensional (3D) chaotic system synchronization was introduced [13]. A wavelet dual function-link fuzzy BELC design for non-linear chaotic systems [14]. Huynh *et al.* presented a modified function-link fuzzy CMAC for chaotic systems [15].

So far, information security is one of the important problems in human life, some areas need to use highly secure communication such as the military, telecommunication, personal

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

information, etc. To perform that, message communication needs to be encrypted and decrypted. The use of chaotic system synchronization for secure communication is one of the methods that has been gaining interest in academic research. With the fast increasing speed of the internet, digital images sent over public networks and the shared network is constantly growing. Digital image security has become an important issue of great concern because the personal information contained in images can be illegally intercepted, processed, and destroyed. Image encoding is a useful way to secure image transmission. The transmission is synchronized with a chaotic system to obtain higher security. Then, the decryption is applied to have the original image again at the received channel. Some remarkable studies can be mentioned as a disposable keys-based lossless dual-channel audio encoding method was introduced, in which a chaotic system with many uncertain coils to produce the keystream is intended to diffuse and mix audio signal to produce a more random chaotic trajectory [16]. An audio coding system based on cosine numerical transformations has been proposed. The transformation is used recursively for sample blocks of uncompressed digital audio signals. Blocks are chosen by using a simple overlapping law to diffuse the encrypted data to every processed block [17]. A method of encoding and decoding voice based on the chaotic transducer has been introduced, in which voice signals are sampled and classified into four levels, and each level of sampled value is permuted by four mixers [18]. Shanmugam *et al.* presented an adaptive control system using adaptive laws to warrant the synchronization for a reactive-diffusive neural network (RDNN). The RDNN with appropriate parameters is selected as a cryptographic system for image secure communication [19]. A 3D chaotic system was applied for signal encoding, in which a real circuit was applied to generate a random number generator, and two optimization methods for system parameters are used to obtain chaotic model parameters from the real chaos circuit [20]. Chang *et al.* introduced an audio encoding method using a digitally programmable multiple scroll chaotic system, in which the number of scrolls can be programmable and changeable in real-time [21]. Man *et al.* introduced a segmented image encryption algorithm using a hybrid chaotic system. An original image is separated into two blocks according to the chaotic and shuffled segmentation method by swapping pixels in the intra-blocks and the inter-blocks [22]. Kalpana *et al.* introduced an audio encoding method using coherent two-way fusion memory synchronization and fuzzy cellular NN with time delays [23]. An image compression and encoding method using a backpropagation NN and a hyperchaotic system have been suggested. A backpropagation NN is used to compress the image pixel values, and the chaotic series of the memristive hyperchaotic system is applied to diffuse the pixel values [24]. A safe audio transmission method is introduced, combining four different techniques for encoding audio in the same system for even more security. The method is called Deoxyribonucleic acid (DNA) encoding and the proposed method is assessed using various measurements such as signal to noise ratio (SNR), root mean square (RMS), peak signal-to-noise ratio (PSNR), and correlation coefficient [25]. Recently, a chaotic synchronization-based secure communication system using a BELC was proposed. The obtained estimation is used as an observer for synchronizing signals of the transmitter and receiver to efficiently reduce synchronization errors [26]. However, several encryption algorithms can be cryptanalyzed because of weaknesses in terms of security such as a 1D logistic map-based color image encryption method using the low dimensional logistic map with a smaller key space and chaotic series, which reduces the encryption performance [27]. Additionally, some image encryption algorithms introduced in [28] and [29] can be broken with some attacks due to the encryption process has no relationship with the original image and that the same chaotic series is used for different original images. Also, few studies have used the combination of CMAC and BELC to apply for chaotic synchronizations, audio and image secure communications based on 3D chaotic systems.

Based on the above discussions, this study produces a new recurrent cerebellar fuzzy brain emotional learning controller (RCFBC). The proposed method is combined a BELC, a recurrent CMAC, and a fuzzy inference system to create the RCFBC that has the advantages of the recurrent CMAC [30] and the BELC [31] that are (1) Using external feedback via recurrent units, built-in loopback allows the network to remember the system's past states and to learn the system parameters. Based on this feature, recurrent CMAC usually shows quick response and good performance in the presence of uncertainties. (2) Using BELC as a powerful non-linear estimator. Such BELC comprises a sensory network imitating the orbitofrontal cortex and the emotional network relating to the amygdala cortex in a human brain. The BELC gives good performance for dynamic systems, so the total performance of the proposed algorithm is significantly enhanced when the quick responsive capacity of RCMAC is combined with the great non-linear estimate capability of BELC. The RCFBC and a robust compensator concurrently form the hybrid control system for 3D Genesio chaotic synchronization, image secure communication, and audio secure communication. The proposed RCFBC, serving as the main controller, is used for mimicking an ideal controller, and the robust compensator is an auxiliary controller, which is used for decreasing the different errors between the RCFBC and the ideal controller. A Lyapunov function is given to prove the stability system and determine the updation laws of the RCFBC. The simulation results of 3D Genesio chaotic synchronization, image secure communication, and audio secure communication and security analysis indexes, validate the feasibility of the proposed hybrid algorithm. This study proposes a new image encryption algorithm to address some mentioned disadvantages. Some justifications for design decisions can be summarized as follows: The proposed algorithm can improve potential security risks that exist in low-dimensional chaotic systems, increase resistance to some attacks during

transmission, satisfy the use of all replacement images. The performance of the proposed algorithm is examined in root mean square error (RMSE), histogram, information entropy, correlation of pixels, PSNR, and some attack analyses such as differential attack, noise attack, and cropping attack. The analysis results point out that our algorithm gives higher encryption efficiency and better security.

The remainder of this paper is organized as follows. The problem formulation is described in Section 2. Section 3 shows in detail the structure of the recurrent cerebellar fuzzy brain emotional controller system design. The online learning laws and convergent analysis is presented in Section 4. Section 5 gives the numerical simulation examples including synchronization of the 3D Genesio chaotic system, image secure communication using 3D Genesio chaotic synchronization, and secure communication for audio signal using 3D Genesio chaotic synchronization. Finally, Section 6 is the conclusion.

II. PROBLEM FORMULATION

A 3-dimensional (3D) chaotic system is defined including a master-slave system. A general 3D master system is given as follows:

$$\begin{cases} \dot{x}_1(t) = f_{MS1}(x_1(t), x_2(t), x_3(t)) \\ \dot{x}_2(t) = f_{MS2}(x_1(t), x_2(t), x_3(t)) \\ \dot{x}_3(t) = f_{MS3}(x_1(t), x_2(t), x_3(t)) \end{cases} \tag{1}$$

where $x_i(t)$, for $i = 1,2$, and 3, is the master system's state and $f_{MSi}(x_1(t), x_2(t), x_3(t))$ is non-linear functions.

A general slave system is defined as follows:

$$\begin{cases} \dot{y}_1(t) = f_{SS1}(y_1(t), y_2(t), y_3(t)) + \Delta f_{SS1}(y_1(t), y_2(t), y_3(t)) \\ \qquad +\delta_1(t) + u_1(t) \\ \dot{y}_2(t) = f_{SS2}(y_1(t), y_2(t), y_3(t)) + \Delta f_{SS2}(y_1(t), y_2(t), y_3(t)) \\ \qquad +\delta_2(t) + u_2(t) \\ \dot{y}_3(t) = f_{SS3}(y_1(t), y_2(t), y_3(t)) + \Delta f_{SS3}(y_1(t), y_2(t), y_3(t)) \\ \qquad +\delta_3(t) + u_3(t) \end{cases} \tag{2}$$

where $y_i(t)$, for $i = 1,2$, and 3, is the system state of slave system, $f_{SSi}(y_1(t), y_2(t), y_3(t))$ is non-linear function, $\Delta f_{SSi}(y_1(t), y_2(t), y_3(t))$ is unknown system uncertainty, $\boldsymbol{\delta}(t) \triangleq [\delta_1(t), \delta_2(t), \delta_3(t)]^T$ is the unknown external disturbance and $u_i(t)$ is the control input.

The aim of chaotic synchronization is to produce a suitable control input $\boldsymbol{u}(t) \triangleq [u_1(t), u_2(t), u_3(t)]^T$, so the states of slave system can mimic the states of master system. Therefore, two master-slave systems can be synchronized, it means that $\lim_{t\to\infty} |\boldsymbol{y}_i(t) - \boldsymbol{x}_i(t)| \to 0$, for $i = 1,2$, and 3.

The proposed algorithm can be applied for some chaotic systems, such as Genesio, Lorentz, Hennon map, and hyper chaotic systems. The reasons for choosing the Genesio chaotic system in our work are summarized as follows: (1) It has three dimensions including a simple square part and three simple ordinary differential equations that depend on three positive real parameters, so it is simple to implement by software and hardware; (2) It has complex dynamical behaviors containing period-doubling bifurcations, chaos, periodic windows, and coexistence of multiple attractors that make it hard to crack; (3) By using different initial conditions and system parameters, its synchronization has given different results. Thus, it is difficult to cryptanalyze if one does not know exactly the initial conditions and system parameters; (4) Its chaotic ranges are wider than some low dimensional maps, so it has a larger secret key space; (5) It has satisfied the randomness test results shown in the Appendix.

The master system of the 3D Genesio chaotic system is expressed as [32]:

$$\begin{cases} \dot{x}_1(t) = x_2(t) \\ \dot{x}_2(t) = x_3(t) \\ \dot{x}_3(t) = -a_S x_1(t) - b_S x_2(t) - c_S x_3(t) + x_1^2(t) \end{cases} \tag{3}$$

where a_S, b_S, c_S are known parameters.

The slave system is given as

$$\begin{cases} \dot{y}_1(t) = y_2(t) + \Delta f_{SS1}(y_1(t), y_2(t), y_3(t)) \\ \qquad +\delta_1(t) + u_1(t) \\ \dot{y}_2(t) = y_3(t) + \Delta f_{SS2}(y_1(t), y_2(t), y_3(t)) \\ \qquad +\delta_2(t) + u_2(t) \\ \dot{y}_3(t) = -a_S y_1(t) - b_S y_2(t) - c_S y_3(t) + y_1^2(t) \\ \qquad +\Delta f_{SS3}(y_1(t), y_2(t), y_3(t)) + \delta_3(t) + u_3(t) \\ = \boldsymbol{f}_{SS}(y_1(t), y_2(t), y_3(t)) + \Delta f_{SS3}(y_1(t), y_2(t), y_3(t)) \\ \qquad +\delta_3(t) + u_3(t) \end{cases} \tag{4}$$

where $y_i(t)$ is the slave system's state, $\Delta f_{SSi}(y_1(t), y_2(t), y_3(t))$ is the unknown uncertainty, $d_i(t)$ is the unknown external disturbance, $\boldsymbol{u}(t) = [u_1(t), u_2(t), u_3(t)]^T$ is the vector of control inputs, and. $\boldsymbol{f}_{SS}(y_1, y_2, y_3) = -a_S y_1(t) - b_S y_2(t) - c_S y_3(t) + y_1^2(t)$.

Define the tracking error function

$$\begin{cases} \dot{e}_1(t) = y_1(t) - x_1(t) \\ \dot{e}_2(t) = y_2(t) - x_2(t) \\ \dot{e}_3(t) = y_3(t) - x_3(t) \end{cases} \tag{5}$$

The error dynamics are then calculated as

$$\begin{cases} \dot{e}_1(t) = \dot{y}_1(t) - \dot{x}_1(t) = e_2(t) + \Delta f_{SS1}(y_1(t), y_2(t), y_3(t)) \\ \qquad +\delta_1(t) + u_1(t) \\ \dot{e}_2(t) = \dot{y}_2(t) - \dot{x}_2(t) = e_3(t) + \Delta f_{SS2}(y_1(t), y_2(t), y_3(t)) \\ \qquad +\delta_2(t) + u_2(t) \\ \dot{e}_3(t) = \dot{y}_3(t) - \dot{x}_3(t) = -a_S e_1(t) - b_S e_2(t) \\ \qquad -c_S e_3(t) + y_1^2(t) - x_1^2(t) \\ \qquad +\Delta f_{SS3}(y_1(t), y_2(t), y_3(t)) + \delta_3(t) + u_3(t) \end{cases} \tag{6}$$

Rewriting (6) by the vector form, obtains

$$\dot{\boldsymbol{e}}(t) = \boldsymbol{H}\boldsymbol{e}(t) + \boldsymbol{f}_{SS}(y_1(t), y_2(t), y_3(t)) + \Delta\boldsymbol{f}_{SS}(y_1(t), y_2(t), y_3(t)) + \boldsymbol{\delta}(t) + \boldsymbol{u}(t) \quad (7)$$

where

$$\boldsymbol{e}(t) = [e_1(t), e_2(t), e_3(t)]^T,$$
$$\boldsymbol{H} = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ -a_S & -b_S & -c_S \end{bmatrix},$$
$$\boldsymbol{f}_{SS}(t) = \begin{bmatrix} 0 \\ 0 \\ y_1^2(t) - x_1^2(t) \end{bmatrix},$$
$$\Delta\boldsymbol{f}_{SS}(y_1(t), y_2(t), y_3(t)) = [\Delta f_{SS1}, \Delta f_{SS2}, \Delta f_{SS3}]^T,$$
$$\boldsymbol{\delta}(t) = [\delta_1(t), \delta_2(t), \delta_3(t)]^T.$$

Define:

$$\bar{\boldsymbol{e}}(t) = [\boldsymbol{e}(t), \dot{\boldsymbol{e}}(t)]^T \quad (8)$$

Then define:

$$\boldsymbol{s}(t) \triangleq \boldsymbol{\theta}_1\boldsymbol{e}(t) + \boldsymbol{\theta}_2 \int_0^t \boldsymbol{e}(t)dt \quad (9)$$
$$\Rightarrow \dot{\boldsymbol{s}}(t)\boldsymbol{\theta}_1\dot{\boldsymbol{e}}(t) + \boldsymbol{\theta}_2\boldsymbol{e}(t) \quad (10)$$

where $\boldsymbol{s}(t)$ is the input variables of the proposed RCFBC, $\boldsymbol{\theta}_1$ and $\boldsymbol{\theta}_2$ are positive diagonal matrices. Set $\boldsymbol{\Theta} = [\boldsymbol{\theta}_2\boldsymbol{\theta}_1]$ is the feedback gain vector. For the reachability and existence of sliding surface $\boldsymbol{s}(t)$, the control effort must satisfy the following inequation

$$\frac{1}{2}\frac{d}{dt}(\boldsymbol{s}_i^T(t)\boldsymbol{s}_i(t)) \le -\sum_{i=1}^{3}\sigma_i|s_i(t)| \quad (11)$$

for $\sigma_i > 0$, with $i = 1, 2$, and 3.

Substituting (10) into (11), obtains

$$\boldsymbol{s}^T(t)\dot{\boldsymbol{s}}(t) = \boldsymbol{s}^T(t)[\ddot{\boldsymbol{e}}(t) + \boldsymbol{\theta}_1\dot{\boldsymbol{e}}(t) + \boldsymbol{\theta}_2\boldsymbol{e}(t)] \le -\sum_{i=1}^{3}\sigma_i|s_i| \quad (12)$$

In case the external disturbances and system dynamics are precisely known, an ideal sliding mode controller can be designed as follows:

$$\boldsymbol{u}^*(t) = -\boldsymbol{H}\boldsymbol{e}(t) - \boldsymbol{f}_{SS}(t) - \boldsymbol{\Theta}\bar{\boldsymbol{e}}(t) - \Delta\boldsymbol{f}_{SS}(y_1(t), y_2(t), y_3(t)) - \boldsymbol{\delta}(t) + \sigma\,\mathrm{sgn}(\boldsymbol{s}(t)) \quad (13)$$

where $sgn(\cdot)$ is a sign function.

Inserting (13) into (7), obtains

$$\dot{\boldsymbol{e}}(t) + \boldsymbol{\Theta}\bar{\boldsymbol{e}}(t) - \sigma\,\mathrm{sgn}(\boldsymbol{s}(t)) = 0 \quad (14)$$

If $\boldsymbol{\Theta}$ is selected to allow the eigenvalues of (14) being in the left-half plane, then $\lim_{t\to\infty}\bar{\boldsymbol{e}}(t) \to 0$. However, the ideal sliding mode control in (13) cannot be obtained. Hence, in the following section, the proposed RCFBC system is applied to attain the chaotic synchronization performance.

III. RECURRENT CEREBELLAR FUZZY BRAIN EMOTIONAL CONTROLLER SYSTEM DESIGN

In order to perfectly synchronize the 3D Genesio chaotic system, a FBELC network is combined with a RCMAC network, it is called as recurrent cerebellar fuzzy brain emotional controller (RCFBC), and its architecture is illustrated in Fig. 1. The RCFBC and a robust compensator concurrently form the hybrid control system for 3D Genesio chaotic synchronization, image secure communication, and audio secure communication.

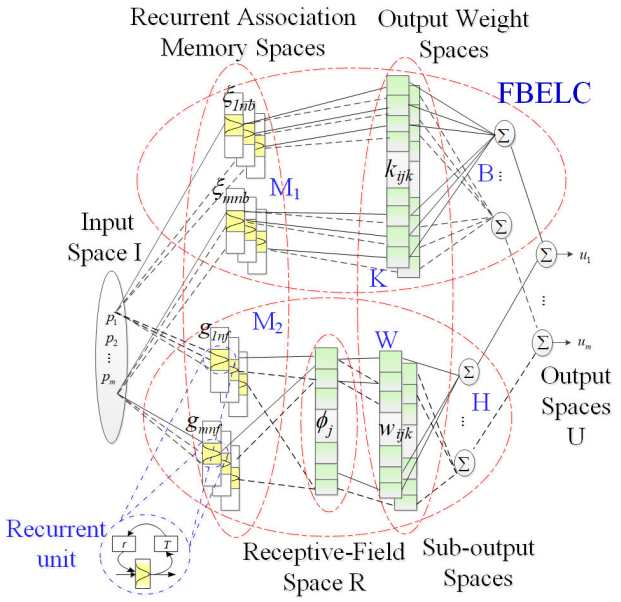


FIGURE 1. The architecture of the proposed RCFBC.

The FBELC contains four spaces that are the input (I), Recurrent association memory (M_1), output weight (K), and sub-output (B). In addition, RCMAC has five spaces that are input (I), recurrent association memory (M_2), receptive-field (R), output weight (W), and sub-output (H). The FBELC outputs subtract the RCMAC outputs to produce the output space (U). The propagation of the signal

from the input space to the output space is described as:

$$\begin{cases} \text{FBLEC network:} I \to M_1 \to K \to B \to U \\ \text{RCMAC network:} I \to M_2 \to R \to W \to H \to U \end{cases}$$

Detailed descriptions for each space of FBELC and RCMAC are defined as follows:

A. INPUT SPACE (I)

An input vector, $\boldsymbol{p} = [p_1 \ldots p_i \ldots p_m]^T \in \Re^m$ with (i = 1,2,…, m), is simultaneously provided to both FBELC and RCMAC; where i is an input index and m is the input dimension.

B. RECURRENT ASSOCIATION MEMORY SPACES (M_1 AND M_2)

M_1 and M_2 comprise respectively some blocks n_b for FBELC and n_f for RCMAC, in which n_b and n_f are the dimensions of the FBELC's block and the RCMAC's block, respectively. Each block is expressed by a Gaussian membership basis function ξ_{ij}. ξ_{ij} is used for FBELC, which is determined by:

$$\xi_{ij} = \exp\left[-\frac{(p_{b_{ij}} - c_{ij})^2}{v_{ij}^2}\right] \tag{15}$$

where v_{ij} and c_{ij} are respectively variance and mean of FBELC, $j = 1,2,\ldots, n_b$. In this space, $p_{b_{ij}}$ is the input of the FBELC.

Set

$$\Xi = [\xi_{11}...\xi_{1n_b}...\xi_{m1}...\xi_{mn_b}]^T \in \Re^{mn_b} \tag{16}$$

Moreover, g_{ij} is a Gaussian membership basis function of RCMAC, which is calculated by:

$$g_{ij} = \exp\left[-\frac{(p_{b_{ij}} - y_{ij})^2}{z_{ij}^2}\right], \tag{17}$$

where z_{ij} and y_{ij} are respectively variance and mean of RCMAC.

For RCMAC network, each input contains two parts that are the present input $p_i(t)$ at time t and the recurrent unit output at time $t - T$ (T is a time unit). Therefore, $p_{g_{ij}}$ is the overall input of the RCMAC, which is determined by:

$$P_{g_{ij}}(t) = P_i(t) + r_{ij}g_{ij}(t - T), \tag{18}$$

where r_{ij} is the recurrent constants for RCMAC.

C. RECEPTIVE FIELD SPACE OF RCMAC (R)

Every element in the receptive-field space ϕ_j is the sum of the corresponding elements of recurrent association memory of RCMAC (M_2), which is calculated as:

$$\phi_j = \sum_{i=1}^{m} g_{ij} = \sum_{i=1}^{m} \exp\left[\frac{-(p_{g_{ij}} - y_{ij})^2}{z_{ij}^2}\right]$$

$$= \exp\left[-\sum_{i=1}^{m} \frac{(p_{g_{ij}} - y_{ij})^2}{z_{ij}^2}\right] \tag{19}$$

Then, define $\boldsymbol{\Phi}$ as:

$$\boldsymbol{\Phi} = [\phi_{11}...\phi_{1n_f}...\phi_{m1}...\phi_{mn_f}]^T \in \Re^{mn_f}.$$

D. OUTPUT WEIGHT SPACES (W AND K)

ω_{ijk} and k_{ijk} are respectively the weights of the RCMAC and the FBELC for i-th output, j-th layer, and k-th block. Then, $\boldsymbol{K}$ is expressed as:

$$\boldsymbol{K} = [k_{1jk}, k_{2jk}...., k_{ijk}, \ldots, k_{mjk}]$$

$$= \begin{bmatrix} k_{111} & k_{211} & \ldots & k_{m11} \\ \vdots & \vdots & & \vdots \\ k_{11n_b} & k_{21n_b} & \ldots & k_{m1n_b} \\ k_{121} & k_{221} & \ldots & k_{m21} \\ \vdots & \vdots & & \vdots \\ k_{12n_b} & k_{22n_b} & \ldots & k_{m2n_b} \\ \vdots & \vdots & & \vdots \\ k_{1m1} & k_{2m1} & \ldots & k_{mm1} \\ \vdots & \vdots & & \vdots \\ k_{1mn_b} & k_{2mn_b} & \ldots & k_{mmn_b} \end{bmatrix} \in \Re^{mn_b \times m} \tag{20}$$

$\boldsymbol{W}$ is defined by:

$$\boldsymbol{W} = [\omega_{1jk}...\omega_{ijk}...\omega_{mjk}]$$

$$= \begin{bmatrix} \omega_{111} & \omega_{211} & \ldots & \omega_{m11} \\ \vdots & \vdots & & \vdots \\ \omega_{11n_f} & \omega_{21n_f} & \ldots & \omega_{m1n_f} \\ \omega_{121} & \omega_{221} & \ldots & \omega_{m21} \\ \vdots & \vdots & & \vdots \\ \omega_{12n_f} & \omega_{22n_f} & \ldots & \omega_{m2n_f} \\ \vdots & \vdots & & \vdots \\ \omega_{1m1} & \omega_{2m1} & \ldots & \omega_{mm1} \\ \vdots & \vdots & & \vdots \\ \omega_{1mn_f} & \omega_{2mn_f} & \ldots & \omega_{mmn_f} \end{bmatrix} \in \Re^{mn_f \times m} \tag{21}$$

E. SUB-OUTPUT SPACES (H AND B)

h_i and b_i are respectively the i-th output for RCMAC and FBELC, which are determined by:

$$h_i = \sum_{j=1}^{m} \sum_{k=1}^{n_f} \omega_{ijk}\phi_{jk} \tag{22}$$

$$b_i = \sum_{j=1}^{m} \sum_{k=1}^{n_b} k_{ijk}\xi_{jk} \tag{23}$$

Define the output vectors $\boldsymbol{h}$ and $\boldsymbol{b}$ as

$$\boldsymbol{h} = [h_1...h_i...h_m]^T = \boldsymbol{W}^T\boldsymbol{\Phi} \tag{24}$$

$$\boldsymbol{b} = [b_1...b_i...b_m]^T = \boldsymbol{K}^T\boldsymbol{\Xi} \tag{25}$$

F. OUTPUT SPACE (U)

The RCFBC's output is the difference between the FBELC's output and RCMAC's output, which is calculated as

$$u_i = b_i - h_i = \sum_{j=1}^{m} \sum_{k=1}^{n_b} k_{ijk}\xi_{jk} - \sum_{j=1}^{m} \sum_{k=1}^{n_f} \omega_{ijk}\phi_{jk} \tag{26}$$

The final output of the entire network is determined by:

$$\boldsymbol{u} = \boldsymbol{b} - \boldsymbol{h} = \boldsymbol{K}^T\boldsymbol{\Xi} - \boldsymbol{W}^T\boldsymbol{\Phi} \tag{27}$$

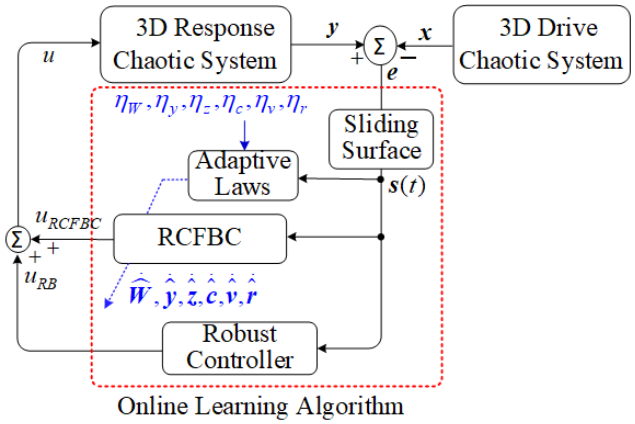


FIGURE 2. Block diagram for synchronization of 3D chaotic systems using the RCFBC.

IV. ONLINE LEARNING LAWS AND CONVERGENT ANALYSIS

A block diagram for the synchronization of 3D chaotic systems using the proposed RCFBC is drawn in Fig. 2. Fig. 2 is a block diagram for the synchronization of 3D chaotic systems, in which the block RCFBC denotes the architecture of Fig. 1; and it shows how the proposed control system can control the 3D response chaotic system to follow the 3D drive chaotic system with trajectory synchronization. It is assumed that there exist an optimal RCFBC, $\boldsymbol{u}^*_{RCFBC}$, to mimic the ideal controller $\boldsymbol{u}^*$ in (13). $\boldsymbol{\varepsilon}$ is a vector of minimum error between the ideal controller and the RCFBC. $\boldsymbol{K}^*$ and $\boldsymbol{W}^*$ are optimal weight matrices of the optimal RCFBC. The ideal sliding mode controller in (13) can be rewritten as:

$$\begin{aligned}\boldsymbol{u}^* &= \boldsymbol{u}^*_{RCFBC} + \boldsymbol{\varepsilon} = (\boldsymbol{b}-\boldsymbol{h})^* + \boldsymbol{\varepsilon} = (\boldsymbol{K}^T\boldsymbol{\Xi} - \boldsymbol{W}^T\boldsymbol{\Phi})^* + \boldsymbol{\varepsilon} \\ &= \boldsymbol{K}^{*T}\boldsymbol{\Xi}^* - \boldsymbol{W}^{*T}\boldsymbol{\Phi}^* + \boldsymbol{\varepsilon} \end{aligned} \tag{28}$$

The RCFBC's output is $\boldsymbol{u}$ and the outputs of FBELC and RCMAC are respectively $\boldsymbol{b}$ and $\boldsymbol{h}$. Since $\boldsymbol{K}^*$, $\boldsymbol{\Xi}^*$, $\boldsymbol{W}^*$, and $\boldsymbol{\Phi}^*$ cannot be precisely obtained in reality, the estimated controller is then defined by:

$$\hat{\boldsymbol{u}} = \hat{\boldsymbol{u}}_{RCFBC} + \boldsymbol{u}_{RB} = \hat{\boldsymbol{K}}^T\hat{\boldsymbol{\Xi}} - \hat{\boldsymbol{W}}^T\hat{\boldsymbol{\Phi}} + \boldsymbol{u}_{RB} \tag{29}$$

Subtracting (13) from (7) and using (10), obtains

$$\dot{\boldsymbol{s}}(t) = \boldsymbol{u}^* - \boldsymbol{u} - \sigma\, sgn(\boldsymbol{s}(t)) \tag{30}$$

Substituting (28) and (29) into (30), yields

$$\begin{aligned}\dot{\boldsymbol{s}}(t) &= [\boldsymbol{K}^{*T}\boldsymbol{\Xi}^* - \boldsymbol{W}^{*T}\boldsymbol{\Phi}^* + \boldsymbol{\varepsilon} - \hat{\boldsymbol{K}}^T\hat{\boldsymbol{\Xi}} + \hat{\boldsymbol{W}}^T\hat{\boldsymbol{\Phi}} - \boldsymbol{u}_{RB}] \\ &\quad -\sigma\,\mathrm{sgn}[\boldsymbol{s}(t)] \\ &= [\tilde{\boldsymbol{K}}^T\boldsymbol{\Xi}^* + \hat{\boldsymbol{K}}^T\tilde{\boldsymbol{\Xi}} - \tilde{\boldsymbol{W}}^T\boldsymbol{\Phi}^* - \hat{\boldsymbol{W}}^T\tilde{\boldsymbol{\Phi}} + \boldsymbol{\varepsilon} - \boldsymbol{u}_{RB}] \\ &\quad -\sigma\,\mathrm{sgn}[\boldsymbol{s}(t)] \end{aligned} \tag{31}$$

where $\tilde{\boldsymbol{\Phi}} = \Phi^* - \hat{\boldsymbol{\Phi}}$, $\tilde{\boldsymbol{K}} = \boldsymbol{K}^* - \hat{\boldsymbol{K}}$, $\tilde{\Xi} = \Xi^* - \hat{\Xi}$, and $\tilde{\boldsymbol{W}} = \boldsymbol{W}^* - \hat{\boldsymbol{W}}$. A partial linear form of $\tilde{\boldsymbol{\Xi}}$ in Taylor series is determined as:

$$\begin{aligned}\tilde{\Xi} &= \begin{bmatrix}\tilde{\xi}_1 \\ \vdots \\ \tilde{\xi}_{n_d}\end{bmatrix} = \begin{bmatrix}\left(\frac{\partial\tilde{\xi}_1}{\partial c}\right)^T \\ \vdots \\ \left(\frac{\partial\tilde{\xi}_{n_d}}{\partial c}\right)^T\end{bmatrix}\Big|_{c=\hat{c}}(c^*-\hat{c}) \\ &\quad + \begin{bmatrix}\left(\frac{\partial\tilde{\xi}_1}{\partial c}\right)^T \\ \vdots \\ \left(\frac{\partial\tilde{\xi}_{n_d}}{\partial c}\right)^T\end{bmatrix}\Big|_{v=\hat{v}}(v^*-\hat{v}) + \beta_1 \\ &= \boldsymbol{\Xi}_c\tilde{c} + \boldsymbol{\Xi}_v\tilde{v} + \boldsymbol{\beta}_1, \end{aligned} \tag{32}$$

where Ξ_c and Ξ_v are defined by:

$$\begin{cases}\Xi_c = \left[\frac{\partial\xi_1}{\partial c}, \quad \cdots \quad, \frac{\partial\xi_{n_d}}{\partial c}\right]^T\Big|_{c=\hat{c}} \in \Re^{n_d\times n_b n_d}, \\ \qquad (n_d = mn_b) \\ \Xi_v = \left[\frac{\partial\xi_1}{\partial v}, \quad \cdots \quad, \frac{\partial\xi_{n_d}}{\partial v}\right]^T\Big|_{v=\hat{v}} \in \Re^{n_d\times n_b n_d}\end{cases} \tag{33}$$

where $\tilde{c} = c^* - \hat{c}$, $\tilde{v} = v^* - \hat{v}$. Rewriting (33) with $\tilde{\Xi} = \Xi^* - \hat{\Xi}$, gives:

$$\Xi^* = \hat{\Xi} + \tilde{\Xi} = \hat{\Xi} + \Xi_c\tilde{c} + \Xi_v\tilde{v} + \boldsymbol{\beta}_1 \tag{34}$$

where $\boldsymbol{\beta}_1$ is a higher-order vector.

Similarly, a partial linear form of $\tilde{\boldsymbol{\Phi}}$ in Taylor series is determined as:

$$\begin{aligned}\tilde{\boldsymbol{\Phi}} &= \begin{pmatrix}\tilde{\phi}_1 \\ \vdots \\ \tilde{\phi}_{n_d}\end{pmatrix} = \begin{pmatrix}(\frac{\partial\phi_1}{\partial y})^T \\ \vdots \\ (\frac{\partial\phi_{n_d}}{\partial y})^T\end{pmatrix}\Big|_{y=\hat{y}}(y^*-\hat{y}) \\ &\quad + \begin{pmatrix}(\frac{\partial\phi_1}{\partial z})^T \\ \vdots \\ (\frac{\partial\phi_{n_d}}{\partial z})^T\end{pmatrix}\Big|_{z=\hat{z}}(z^*-\hat{z}) \\ &\quad + \begin{pmatrix}(\frac{\partial\phi_1}{\partial r})^T \\ \vdots \\ (\frac{\partial\phi_{n_d}}{\partial r})^T\end{pmatrix}\Big|_{r=\hat{r}}(r^*-\hat{r}) + \beta_2 \\ &= \tilde{\boldsymbol{\Phi}}_y\tilde{y} + \tilde{\boldsymbol{\Phi}}_z\tilde{z} + \tilde{\boldsymbol{\Phi}}_r\tilde{r} + \boldsymbol{\beta}_2 \end{aligned} \tag{35}$$

where $\boldsymbol{\Phi}_y$, $\boldsymbol{\Phi}_z$ and $\boldsymbol{\Phi}_r$ are defined by:

$$\begin{cases} \boldsymbol{\Phi}_y = \left[\dfrac{\partial \phi_1}{\partial y}, \quad \cdots \quad , \dfrac{\partial \phi_{n_d}}{\partial y} \right]^T \Big|_{y=\hat{y}} \in \Re^{n_d \times n_f n_d} \\ \boldsymbol{\Phi}_z = \left[\dfrac{\partial \phi_1}{\partial z}, \quad \cdots \quad , \dfrac{\partial \phi_{n_d}}{\partial z} \right]^T \Big|_{z=\hat{z}} \in \Re^{n_d \times n_f n_d} \\ \boldsymbol{\Phi}_r = \left[\dfrac{\partial \phi_1}{\partial r}, \quad \cdots \quad , \dfrac{\partial \phi_{n_d}}{\partial r} \right]^T \Big|_{r=\hat{r}} \in \Re^{n_d \times n_f n_d} , \end{cases} \tag{36}$$

where $\tilde{\boldsymbol{y}} = \boldsymbol{y}^* - \hat{\boldsymbol{y}}, \tilde{\boldsymbol{z}} = \boldsymbol{z}^* - \hat{\boldsymbol{z}}, \tilde{\boldsymbol{r}} = \boldsymbol{r}^* - \hat{\boldsymbol{r}}$. Rewriting (35) with $\tilde{\boldsymbol{\Phi}} = \Phi^* - \hat{\boldsymbol{\Phi}}$, gives

$$\boldsymbol{\Phi}^* = \hat{\boldsymbol{\Phi}} + \tilde{\boldsymbol{\Phi}} = \tilde{\boldsymbol{\Phi}}_y \tilde{y} + \tilde{\boldsymbol{\Phi}}_z \tilde{z} + \tilde{\boldsymbol{\Phi}}_r \tilde{r} + \boldsymbol{\beta}_2 \tag{37}$$

where $\boldsymbol{\beta}_2$ is a higher-order vector.

Substituting (34) and (37) to (31), Eq. (31) is rewritten as:

$$\begin{aligned} \dot{\boldsymbol{s}}(t) = & [\tilde{\boldsymbol{K}}^T (\hat{\Xi} + \Xi_c \tilde{\boldsymbol{c}} + \Xi_v \tilde{\boldsymbol{v}} + \boldsymbol{\beta}_1) \\ & + \hat{\boldsymbol{K}}^T (\Xi_c \tilde{\boldsymbol{c}} + \Xi_v \tilde{\boldsymbol{v}} + \boldsymbol{\beta}_1) \\ & - \tilde{\boldsymbol{W}}^T (\hat{\boldsymbol{\Phi}} + \boldsymbol{\Phi}_y \tilde{\boldsymbol{y}} + \boldsymbol{\Phi}_z \tilde{\boldsymbol{z}} + \boldsymbol{\Phi}_r \tilde{\boldsymbol{r}} + \boldsymbol{\beta}_2) \\ & - \hat{\boldsymbol{W}}^T (\boldsymbol{\Phi}_y \tilde{\boldsymbol{y}} + \boldsymbol{\Phi}_y \tilde{\boldsymbol{y}} + \boldsymbol{\Phi}_z \tilde{\boldsymbol{z}} + \boldsymbol{\Phi}_r \tilde{\boldsymbol{r}} + \boldsymbol{\beta}_2) \\ & - \hat{\boldsymbol{W}}^T (\boldsymbol{\Phi}_y \tilde{y} + \boldsymbol{\Phi}_z \tilde{z} + \boldsymbol{\Phi}_r \tilde{r} + \boldsymbol{\beta}_2) + \boldsymbol{\varepsilon} - \boldsymbol{u}_{RB}] \\ & - \sigma \operatorname{sgn}[\boldsymbol{s}(t)] \\ = & [\hat{\boldsymbol{K}}^T (\boldsymbol{\Xi}_c \tilde{c} + \boldsymbol{\Xi}_v \tilde{v}) - \hat{\boldsymbol{W}}^T (\boldsymbol{\Phi}_y \tilde{\boldsymbol{y}} + \boldsymbol{\Phi}_z \tilde{\boldsymbol{z}} + \boldsymbol{\Phi}_r \tilde{\boldsymbol{r}}) \\ & + \tilde{\boldsymbol{K}}^T \hat{\boldsymbol{\Xi}} - \tilde{\boldsymbol{W}}^T \hat{\boldsymbol{\Phi}} + \boldsymbol{\tau} - \boldsymbol{u}_{RB}] - \sigma \operatorname{sgn}[\boldsymbol{s}(t)] \end{aligned} \tag{38}$$

where $\boldsymbol{\tau} = \boldsymbol{K}^{*T} \boldsymbol{\beta}_1 + \tilde{\boldsymbol{W}}^T \boldsymbol{\beta}_2 + \tilde{\boldsymbol{K}}^T (\Xi_c \tilde{\boldsymbol{c}} + \Xi_v \tilde{\boldsymbol{v}}) + \tilde{\boldsymbol{W}}^T (\boldsymbol{\Phi}_y \tilde{\boldsymbol{y}} + \boldsymbol{\Phi}_z \tilde{\boldsymbol{z}} + \boldsymbol{\Phi}_r \tilde{\boldsymbol{r}}) + \boldsymbol{\varepsilon}$ is a lumped error for RCMAC, and $\tilde{\boldsymbol{K}} = \boldsymbol{K}^* - \hat{\boldsymbol{K}} = [\hat{k}_1, \hat{k}_2 ... \hat{k}_m]^T \in \Re^{m \times m n_b}$ is an estimation error matrix for the weights of FBELC. A robust compensator [33] is used to estimate for $\boldsymbol{\tau}$ and $\tilde{\boldsymbol{K}}$ as:

$$\begin{aligned} & \sum_{i=1}^{m} \int_0^T s_i^2(t) dt \\ & \leq s^T(0) s(0) + tr[\tilde{W}^T(0) \eta_W^{-1} \tilde{W}(0)] \\ & \quad + \tilde{c}^T(0) \eta_c^{-1} \tilde{c}(0) + \tilde{v}^T(0) \eta_v^{-1} \tilde{v}(0) + \tilde{y}^T(0) \eta_y^{-1} \tilde{y}(0) \\ & \quad + \tilde{z}^T(0) \eta_z^{-1} \tilde{z}(0) + \tilde{r}^T(0) \eta_r^{-1} \tilde{r}(0) \\ & \quad + \sum_{i=1}^{m} \rho_i^2 \int_0^T \tau_i^2(t) dt + \sum_{i=1}^{m} \int_0^T \tilde{k}_i^2(t) dt, \end{aligned} \tag{39}$$

where ρ_i is an attenuation constant, and η_W, η_c, $\eta_v \eta_y$, η_z, and η_r are positive constant learning rates. If the initial conditions are given as $s(0) = 0$, $\tilde{W}(0) = 0$, $\tilde{c}(0) = 0$, $\tilde{v}(0) = 0$, $\tilde{y}(0) = 0$, $\tilde{z}(0) = 0$, $\tilde{r}(0) = 0$, then, (39) is rewritten as:

$$\sum_{i=1}^{m} \int_0^T s_i^2(t) dt \leq \sum_{i=1}^{m} \rho_i^2 \int_0^T \tau_i^2(t) dt + \sum_{i=1}^{m} \int_0^T \tilde{k}_i^2(t) dt, \tag{40}$$

Assume that the approximation error between the proposed RCFBC and an ideal controller are bounded, which means $\tau_i \in L_2(0, T_1)$ and $\tilde{k}_i \in L_2(0, T_2)$, in which $\forall T_1, T_2 \in [0, \infty)$. Thus, $\int_0^T \tau_i^2(t) dt < \chi_1$ and $\int_0^T \tilde{k}_i^2(t) dt < \chi_2$, where χ_1 and χ_2 are large positive constants. If $\sum_{i=1}^{m} \int_0^T s_i^2(t) dt = \infty$, the approximation error will diverge and the control system will be unstable. As a result, the following inequation must be satisfied to allow the stability control system:

$$\sum_{i=1}^{m} \int_0^T s_i^2(t) dt \leq \|\rho_i\|^2 \chi_1 + \chi_2 < \infty \tag{41}$$

The updation laws for the RCFBC and the robust compensator are derived by using a Lyapunov stability function in order to ensure system stability. Thus, the following theorem is produced as:

Theorem 1: The 3D chaotic systems are given in (1) and (2), the adaptive laws for updating the parameters of RCFBC are described from (44) to (49), and the robust compensator is given in (50). Then, the robust system stability can be guaranteed.

$$\dot{\hat{\boldsymbol{K}}} = \alpha [\Xi \times max(0, \boldsymbol{d} - \boldsymbol{b})], \tag{42}$$

$$\boldsymbol{d} = \gamma \times \boldsymbol{p} + \mu \times \boldsymbol{u}_{RCFBC}, \tag{43}$$

where α is a positive learning-rate, $\boldsymbol{d}$ includes the $\boldsymbol{u}_{RCFBC}$ and the $\boldsymbol{p}$ input, γ and μ are positive constants. The updation laws for the parameters of the system are defined as:

$$\dot{\hat{\boldsymbol{W}}} = -\eta_W \hat{\boldsymbol{\Phi}} s^T(t), \tag{44}$$

$$\dot{\hat{\boldsymbol{y}}} = -\eta_y \boldsymbol{\Phi}_y^T \hat{\boldsymbol{W}} s^T(t), \tag{45}$$

$$\dot{\hat{\boldsymbol{z}}} = -\eta_z \boldsymbol{\Phi}_z^T \hat{\boldsymbol{W}} s^T(t), \tag{46}$$

$$\dot{\hat{\boldsymbol{c}}} = \eta_c \Xi_c^T \hat{\boldsymbol{K}} s^T(t), \tag{47}$$

$$\dot{\hat{\boldsymbol{v}}} = \eta_v \Xi_v^T \hat{\boldsymbol{K}} s^T(t), \tag{48}$$

$$\dot{\hat{\boldsymbol{r}}} = -\eta_r \boldsymbol{\Phi}_r^T \hat{\boldsymbol{W}} s^T(t), \tag{49}$$

$$\boldsymbol{u}_{RB} = (2\boldsymbol{Q})^{-1} \left[(I + \Xi^2) \boldsymbol{Q}^2 + \boldsymbol{I} \right] s^T(t), \tag{50}$$

where $\boldsymbol{Q} = diag[\rho_1 \rho_2 \ldots \rho_m] \in \Re^{m \times m}$ is a diagonal attenuation constant matrix for the robust compensator.

Proof: A Lyapunov stability function is chosen by:

$$\begin{aligned} & V(\boldsymbol{s}(t)), \tilde{\boldsymbol{K}}, \tilde{\boldsymbol{W}}, \tilde{\boldsymbol{c}}, \tilde{\boldsymbol{v}}, \tilde{\boldsymbol{y}}, \tilde{\boldsymbol{z}}, \tilde{\boldsymbol{r}}) \\ & = \frac{1}{2} [s^T(t) \boldsymbol{s}(t) + tr[\tilde{\boldsymbol{K}}^T \alpha^{-1} \tilde{\boldsymbol{K}}] \\ & \quad + \tilde{\boldsymbol{c}}^T \eta_c^{-1} \tilde{\boldsymbol{c}} + \tilde{\boldsymbol{v}}^T \eta_v^{-1} \tilde{\boldsymbol{v}} + \tilde{\boldsymbol{y}}^T \eta_y^{-1} \tilde{\boldsymbol{y}} + \tilde{\boldsymbol{z}}^T \eta_z^{-1} \tilde{\boldsymbol{z}} \\ & \quad + \tilde{\boldsymbol{r}}^T \eta_r^{-1} \tilde{\boldsymbol{r}} + tr(\tilde{\boldsymbol{W}}^T \eta_w^{-1} \tilde{\boldsymbol{W}}) \end{aligned} \tag{51}$$

$$\begin{aligned} \Rightarrow & \dot{V}(\boldsymbol{s}(t)), \tilde{\boldsymbol{K}}, \tilde{\boldsymbol{W}}, \tilde{\boldsymbol{c}}, \tilde{\boldsymbol{v}}, \tilde{\boldsymbol{y}}, \tilde{\boldsymbol{z}}, \tilde{\boldsymbol{r}}) = \boldsymbol{s}^T(t) \dot{\boldsymbol{s}}(t) + tr[\tilde{\boldsymbol{K}}^T \alpha^{-1} \dot{\tilde{\boldsymbol{K}}}] \\ & \quad + \tilde{\boldsymbol{c}}^T \eta_c^{-1} \dot{\tilde{\boldsymbol{c}}} + \tilde{\boldsymbol{v}}^T \eta_v^{-1} \dot{\tilde{\boldsymbol{v}}} + \tilde{\boldsymbol{y}}^T \eta_y^{-1} \dot{\tilde{\boldsymbol{y}}} + \tilde{\boldsymbol{z}}^T \eta_z^{-1} \dot{\tilde{\boldsymbol{z}}} + \tilde{\boldsymbol{r}}^T \eta_r^{-1} \dot{\tilde{\boldsymbol{r}}} \\ & \quad - tr(\tilde{\boldsymbol{W}}^T \eta_w^{-1} \dot{\tilde{\boldsymbol{W}}}) \\ & = \boldsymbol{s}^T(t) \tilde{\boldsymbol{K}} \hat{\Xi} - \boldsymbol{s}^T(t) (\tau - \boldsymbol{u}_{RB}) - \boldsymbol{s}^T(t) \hat{\boldsymbol{K}} (\Xi_c \tilde{\boldsymbol{c}} + \Xi_v \tilde{\boldsymbol{v}}) \\ & \quad - \boldsymbol{s}^T(t) \hat{\boldsymbol{W}} (\Phi_y \tilde{\boldsymbol{y}} + \Phi_z \tilde{\boldsymbol{z}} + \Phi_r \tilde{\boldsymbol{r}}) - tr(\tilde{\boldsymbol{K}} \alpha^{-1} \dot{\tilde{\boldsymbol{K}}}) \\ & \quad - \tilde{\boldsymbol{c}}^T \eta_c^{-1} \dot{\tilde{\boldsymbol{c}}} - \tilde{\boldsymbol{v}}^T \eta_v^{-1} \dot{\tilde{\boldsymbol{v}}} - \tilde{\boldsymbol{y}}^T \eta_y^{-1} \dot{\tilde{\boldsymbol{y}}} - \tilde{\boldsymbol{z}}^T \eta_z^{-1} \dot{\tilde{\boldsymbol{z}}} - \tilde{\boldsymbol{r}}^T \eta_r^{-1} \dot{\tilde{\boldsymbol{r}}} \\ & \quad - tr(\tilde{\boldsymbol{W}}^T \eta_w^{-1} \dot{\hat{\boldsymbol{W}}}) + \boldsymbol{s}^T(t) (\tau - \boldsymbol{u}_{RB}) - \boldsymbol{s}^T(t) \sigma \operatorname{sgn}[\boldsymbol{s}(t)] \\ & \leq -tr[\tilde{\boldsymbol{W}}^T \boldsymbol{s}(t) \hat{\Phi} + \eta_w^{-1} \dot{\hat{\boldsymbol{W}}}] + \tilde{\boldsymbol{c}}[\boldsymbol{s}(t) \hat{\boldsymbol{K}} \Xi_c - \eta_c^{-1} \dot{\tilde{\boldsymbol{c}}}] \end{aligned}$$

$$+\tilde{\nu}[s^T(t)\hat{K}\Xi_v - \eta_v^{-1}\dot{\hat{\nu}}] - \tilde{y}[s^T(t)\hat{W}\Phi_y + \eta_y^{-1}\dot{\hat{y}}]$$
$$-\tilde{z}[s^T(t)\hat{W}\Phi_z - \eta_z^{-1}\dot{\hat{z}}] - \tilde{r}[s^T(t)\hat{W}\Phi_r - \eta_r^{-1}\dot{\hat{r}}]$$
$$+s^T(t)\tilde{K}\hat{\Xi} + s^T(t)(\tau - u_{RB}) \quad (52)$$

From (42), if $d_i - b_i \le 0 \Rightarrow \dot{\hat{K}} = 0$. And if $\boldsymbol{d} - \boldsymbol{b} > 0 \Rightarrow \dot{\hat{K}} = \alpha \times \Xi \times [\boldsymbol{d} - \boldsymbol{b}] > 0$. Assume that $\tilde{K} \in L_2[0, T_2] \Rightarrow -tr(\tilde{K}\alpha^{-1}\dot{\hat{K}}) \le 0$. Substituting (44)-(50) into (52), yields:

$$\dot{V}(s(t), \tilde{K}, \tilde{W}, \tilde{c}, \tilde{\nu}, \tilde{y}, \tilde{z}, \tilde{r}) \le s^T(t)\tilde{K}\hat{\Xi} + s^T(t)(\tau - u_{RB})$$
$$= s^T(t)\tilde{K}\hat{\Xi} - \frac{1}{2}\frac{s^T(t)s(t)}{Q^2} - \frac{1}{2}s^T(t)s(t) + s^T(t)\tau$$
$$-\frac{1}{2}s^T(t)s(t)\hat{\Xi}\hat{\Xi}^T$$
$$= -\frac{1}{2}s^T(t)s(t) - \frac{1}{2}\left[\frac{s(t)}{Q} - Q\tau\right]^2 - \frac{1}{2}[s^T(t)\hat{\Xi} - \tilde{K}]^2$$
$$+\frac{1}{2}Q^2\tau^2 + \frac{1}{2}\tilde{K}^T\tilde{K}$$
$$\le -\frac{1}{2}s^T(t)s(t) + \frac{1}{2}Q^2\tau^2 + \frac{1}{2}\tilde{K}^T\tilde{K} \quad (53)$$

Integrating (53) with $t \in [0, T]$, obtains:

$$V(T) - V(0) \le -\frac{1}{2}\sum_{i=1}^{m}\int_0^T s_i^2(t)dt + \frac{1}{2}\sum_{i=1}^{m}\rho_i^2 \times \int_0^T \tau_i^2(t)dt$$
$$+\frac{1}{2}\sum_{i=1}^{m}\int_0^T \tilde{k}_i^2(t)dt \quad (54)$$

where $V(0) > 0$ and $V(T) > 0$, via (39) and (40), it can be concluded that $\sum_{i=1}^{m}\int_0^T s_i^2(t)dt < \infty$ This points out that the increasing error does not diverge, so the total control system is stable. As a result, the stability system is guaranteed.

V. NUMERICAL SIMULATION EXAMPLES

A. SYNCHRONIZATION OF 3D GENESIO CHAOTIC SYSTEM

The dynamic equations for the master-slave systems of 3D Genesio chaotic system are given in (3) and (4). Their initial states and system's parameters are set as

$x(0) = [2, -2, 1]^T$ and $y(0) = [-5, 5, -5]^T$, $\Delta f_{SSi}(y_1(t), y_2(t), y_3(t)) = -0.1 \times y_i(t)$, $\delta(t) = [0.2\cos(2t), 0.1\sin(2\pi t), 0.4\cos(\pi t)]^T$, and $a_S = 6$, $b_S = 2.92$, $c_S = 1.2$. In addition, the initial system parameters are listed in Table 1.

The results for the 3D Genesio master-slave synchronization are shown in Figs. 3-11. The 3D tracking trajectory is plotted in Fig. 3. The 2D tracking trajectories are shown in Figs. 4-6. The comparison of 2D tracking trajectories using RCMAC [34], FBELC [11], and the proposed RCFBC are presented in Figs. 7-9. Tracking errors and the control efforts are respectively presented in Fig. 10 and Fig. 11. Tracking errors of the proposed RCFBC are quickly returned to zero. So, the synchronization results of the RCFBC attain better performance and faster response than other control systems

TABLE 1. Initial parameters of FBELC and RCMAC.

	FBELC	RCMAC
Total of blocks for M_1 and M_2 layers	10	10
Total of blocks for receptive field space R	-	10
Total of blocks for output weight space K and W	10	10
Number of sub-outputs B and H	2	2
The initialization range for mean y_{ij} and c_{ij}	[−1.0, 1.0]	[−1.0, 1.0]
Initial variances z_{ij} and v_{ij}	0.001	0.01
The initialization range for k_{ijk} and ω_{ijk}	[−0.5, 0.5]	[−0.5, 0.5]
Learning rates for α, γ, μ and η_W	0.01, 0.05, 0.01	0.01
Diagonal matrices for robust compensator Q	$Q = 0.05 \times I_{3\times3}$	$Q = 0.05 \times I_{3\times3}$
Learning rates for η_c and η_y	0.0001	0.01
Learning rates for η_v and η_z	0.0001	0.01
Learning-rate of recurrent unit η_r	-	0.01

TABLE 2. Comparisons of computation time and RMSE for RCMAC, FBELC, and RCFBC.

Methods	Computation time (s)	RMSE 1	RMSE 2	RMSE 3	Average RMSE
RCMAC [34]	0.0010	0.2057	0.2705	0.2307	0.2357
FBELC [11]	0.0012	0.2027	0.2225	0.1205	0.1819
RCFBC	**0.0014**	**0.0707**	**0.0804**	**0.0582**	**0.0698**

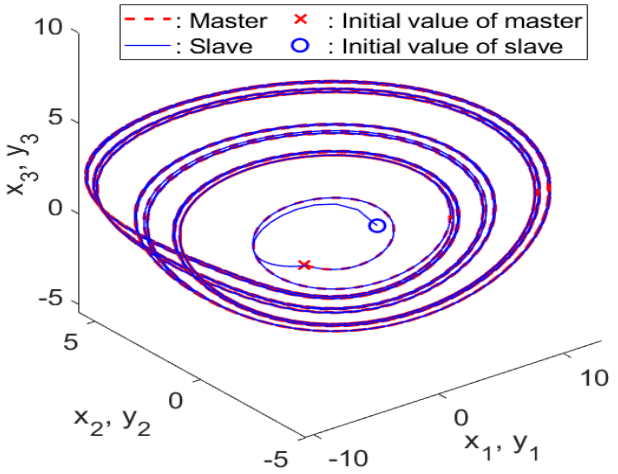


FIGURE 3. 3D tracking trajectories of the Genesio chaotic system using the proposed RCFBC.

even under the effects of external noise and system uncertainties. From the simulation results, the proposed RCFBC synchronize well with smaller tracking errors than the RCMAC and the FBELC (see Table 2). In particular, the RMSE of the RCFBC is reduced by 3.38 times compared to the RCMAC, and 2.61 times compared to the FBELC.

B. IMAGE SECURE COMMUNICATION USING 3D GENESIO CHAOTIC SYNCHRONIZATION

This study proposes a new image encryption algorithm by reducing the value of all pixels of the original image to

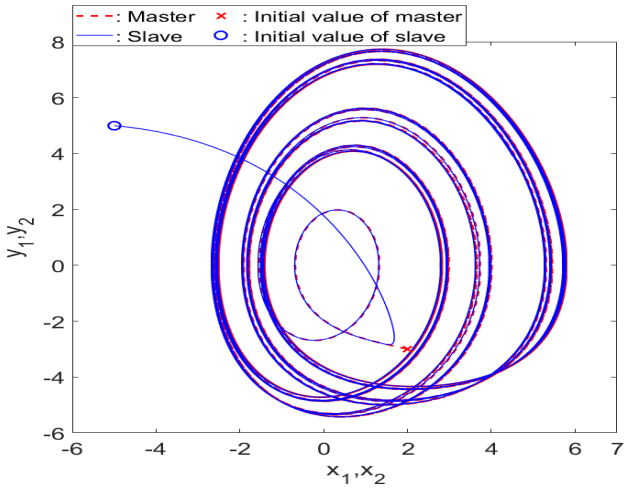


FIGURE 4. 2D tracking trajectories for x_1, x_2 and y_1, y_2 using the proposed RCFBC.

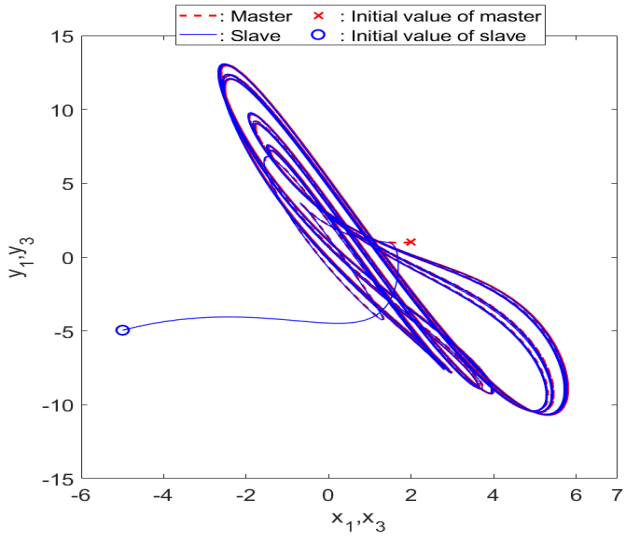


FIGURE 5. 2D tracking trajectories for x_1, x_3 and y_1, y_3 using the proposed RCFBC.

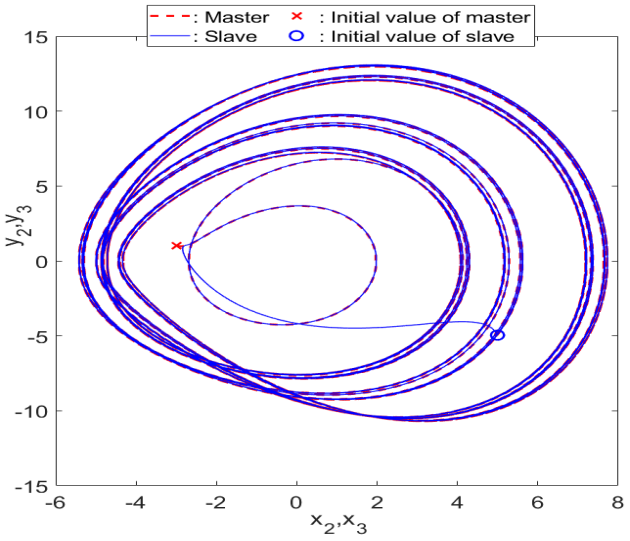


FIGURE 6. 2D tracking trajectories for x_2, x_3 and y_2, y_3 using the proposed RCFBC.

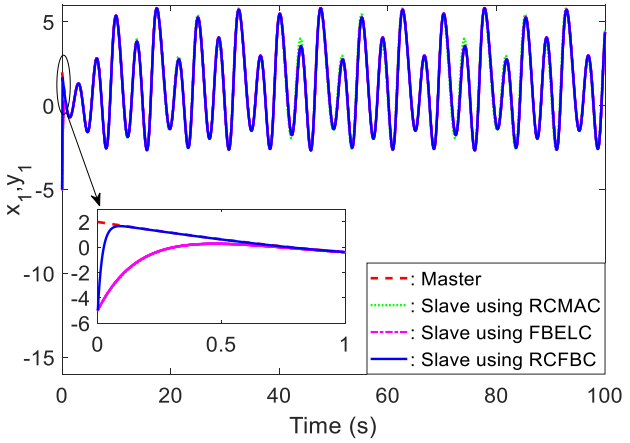


FIGURE 7. Tracking trajectories of x_1 and y_1 using RCMAC, FBELC, and the proposed RCFBC.

improve efficiency and security, in which a mixed image including an original image and a replacement image is used to encrypt and to transmit to the receiver. The image encryption algorithm contains five steps using to combine the original image, the replacement image and the master chaotic system to generate an encrypted image. Then the encrypted image is sent through a public channel. Previously synchronized data using the proposed RCFBC is used to extract the encrypted image at the receiver so that the decryption procedure can then be performed. The decryption procedure has simply applied the reverse of each step of the encryption algorithm to take the decrypted image. The detailed architecture of the image secure communication is presented in Fig. 12. The master system is in the transmitter side and the slave system is in the receiver side. The receiver only needs to know which kind of chaotic system is used in this transmission (for example: the dynamic equations in (3) is known by the receiver side), and does not need to transmit the synchronization information from the transmitter side to receiver side. So, we can choose a lot of chaotic systems, and each transmission uses different chaotic system; then by a prior agreement or send a hidden bit, the receiver side can know which one chaotic system is used. Also, in this study, the replacement image can be chosen by any cover image, however, it should satisfy some specifications as follows: The replacement image must be the same size as the original image and it should be a color image with three red-green-blue (RGB) channels.

1) THE PROPOSED IMAGE ENCRYPTION ALGORITHM

a: ENCRYPTION

Step 1: In order to increase the security for the original image. We use a replacement image (R) to hide the original image inside. It is supposed that the size of the original and the replacement images is a matrix with the same size, then its

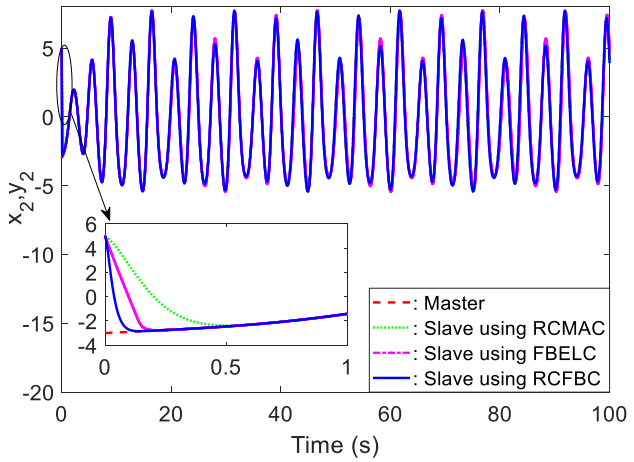


FIGURE 8. Tracking trajectories of x_2 and y_2 using RCMAC, FBELC, and the proposed RCFBC.

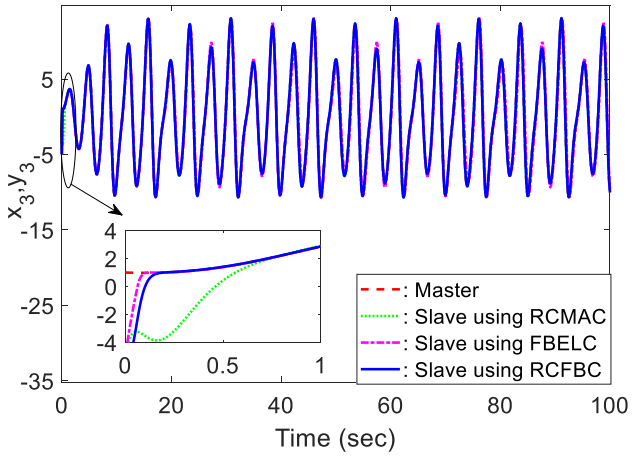


FIGURE 9. Tracking trajectories of x_3 and y_3 using RCMAC, FBELC, and the proposed RCFBC.

pixels can be arranged by the order from top to bottom and left to right to create a decimal set as

$$\boldsymbol{S} = [S_1, S_2, ..., S_{h\times w}] \tag{55}$$

$$\boldsymbol{R} = [R_1, R_2, ..., R_{h\times w}] \tag{56}$$

where h and w are respectively the row and column of the image.

Then, the values of pixels of the original and replacement images are divided into three RGB channels, then they are mixed by using the following equations

$$\boldsymbol{S}_{RGB} = im2double(imread(\boldsymbol{S})) \tag{57}$$

$$\boldsymbol{R}_{RGB} = im2double(imread(\boldsymbol{R})) \tag{58}$$

$$\boldsymbol{DS}_{RGB} = dct2(\boldsymbol{S}_{RGB})) \tag{59}$$

$$\boldsymbol{DR}_{RGB} = dct2(\boldsymbol{R}_{RGB})) \tag{60}$$

$$\boldsymbol{M}_{RGB} = \boldsymbol{DR}_{RGB} + \boldsymbol{\rho} \times \boldsymbol{DS}_{RGB} \tag{61}$$

where *im2double*(.) converts the image to double precision; *dct2*(.) returns the two-dimensional discrete cosine transform; $\boldsymbol{S}_{RGB}$ and $\boldsymbol{R}_{RGB}$ include three RGB channels of the image. $\boldsymbol{\rho}$ is a gain matrix, ($\boldsymbol{\rho} \neq 0$, if $\boldsymbol{\rho} = 0$, the mixed image becomes black and it cannot be recovered in the decryption process). If the $\boldsymbol{\rho}$ value is small, the original image will disappear and hide inside the replacement image. If $\boldsymbol{\rho}$ is chosen large enough, the mixed image becomes white, so both the original image and the replacement image cannot

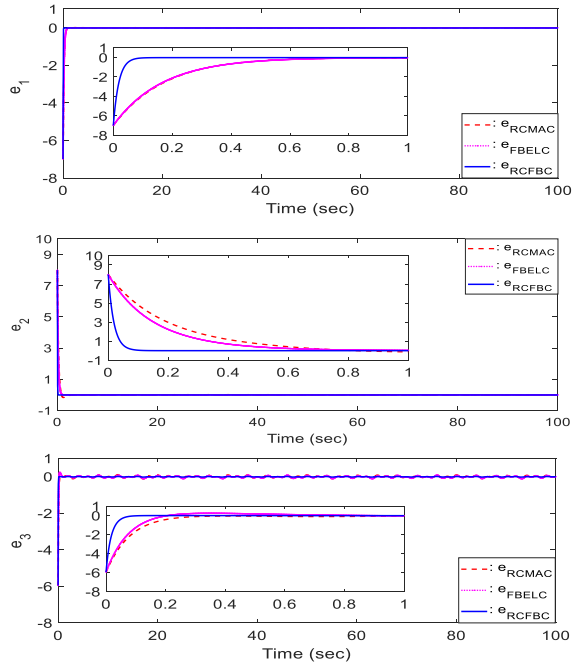


FIGURE 10. Comparision of error signals using RCMAC, FBELC, and RCFBC.

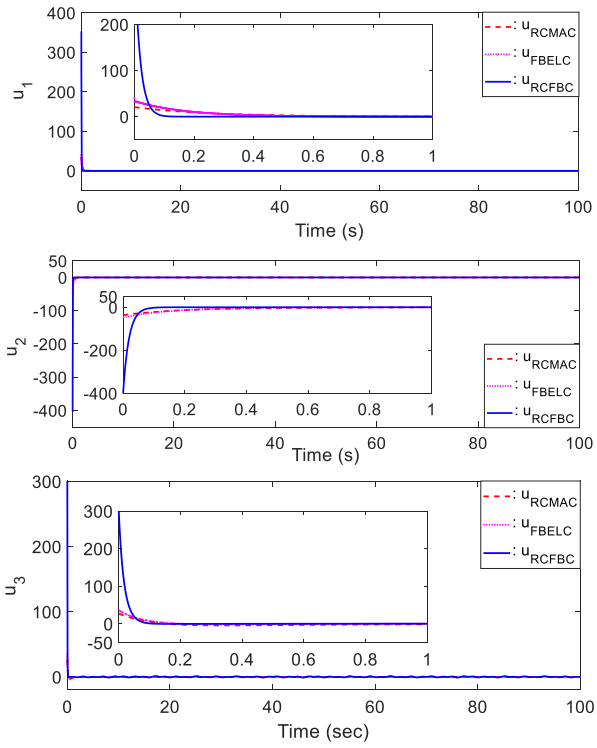


FIGURE 11. Comparision of control signals using RCMAC, FBELC, and RCFBC.

be recognized, it implies that the confidentiality of data is still guaranteed. $\boldsymbol{DS}_{RGB}$ and $\boldsymbol{DR}_{RGB}$ include the discrete cosine transform values of $\boldsymbol{S}_{RGB}$ and $\boldsymbol{R}_{RGB}$; $\boldsymbol{M}_{RGB}$ is the mixed matrix of $\boldsymbol{DS}_{RGB}$ and $\boldsymbol{DR}_{RGB}$.

Step 2: All decimal pixel values of $\boldsymbol{M}_{RGB}$ are then converted to binary numbers and a new set can be obtained as follows

$$\boldsymbol{B} = [B_1, B_2, ..., B_{h\times w}], i = 1 \ldots (h \times w) \tag{62}$$

where B_i is the binary value of the pixel. $i = 1, 2, ..., h \times w$ is the i th iteration of the chaotic system.

Step 3: Discrete the continuous 3D Genesio chaotic system with the fixed step $f_s = 0.001$ and using the Runge–Kutta scheme [35], and repeat continuously for $h \times w$ times. For the encryption, the variables are a double type with a 64 bit-length and a 15-digit precision. The decimal values of the variables are then multiplied by 10^{14}. For each iteration, three values of x_i, y_i, and z_i can be obtained, then these values are processed as follows:

$$C_m(i) = de2bi[round(\ mod\ (abs\ (C_m\ (i)) - floor\ (abs\ (C_m\ (i))) \times 10^{14},\ 256))] \tag{63}$$

where $de2bi(.)$ converts a decimal number to a binary value; $mod\ (x,\ y)$ returns the remainder after division x/y. $floor(x)$ rounds the elements to the nearest integers less than or equal to x. $abs(.)$ gives the absolute value, and $round(.)$ rounds the elements to the nearest integers. And $m = x_i, y_i$, and z_i.

Set $\boldsymbol{C} = [C_m\ (i)\ , i = 1, 2, \ldots, h\times w] = [C_1, C_2, .., C_{h\times w}]$.

Step 4: The scrambled image is then created based on the confusion and diffusion encryption technique as in [36]. Firstly, two types of auxiliary matrices need be defined. $\boldsymbol{I}$ and $\boldsymbol{T}$ are used to determine which pixels are to be processed and $\boldsymbol{D}$ is for diffusion. For an image of size $h \times w$, three random sequences r_1, r_2, and r_3 are used to cut from chaotic sequence $\boldsymbol{C}$ to create two index matrices $\boldsymbol{I}$ and $\boldsymbol{T}$. The following steps are used to obtain $\boldsymbol{I}$ and $\boldsymbol{T}$:

- Arrange r_1, r_2, and r_3 by ascending order to take the sort index si_1, si_2, and si_3, respectively
- Generate $\boldsymbol{I}$ and $\boldsymbol{T}$ using si_1, si_2, and si_3 as follows:

for $i = 1 \rightarrow h$

for $j = 1 \rightarrow w$

$$I(i,j) = si_1\ ((\mathrm{mod}(i + si_1(j) - 1, h) + 1)\ ;$$
$$T(i,j) = si_2\ ((\mathrm{mod}(i + si_3(j) - 1, w) + 1)\ ;$$

end

end

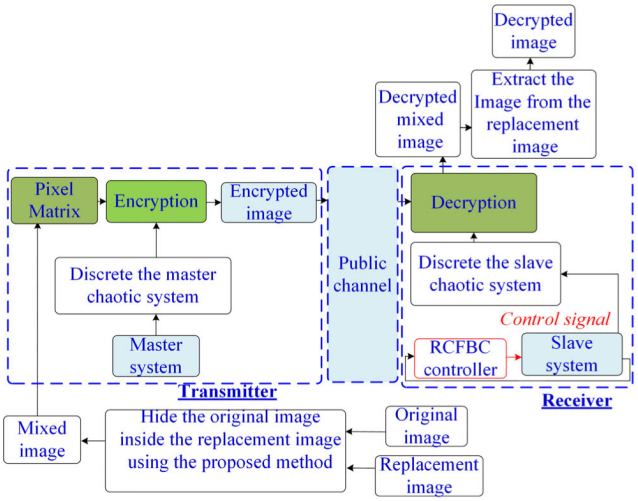


FIGURE 12. The architecture of the image secure communication.

$\boldsymbol{I}$ and $\boldsymbol{T}$ have the same size as the original image. Next, using a random sequence r_4 including $h \times w$ values cut from $\boldsymbol{C}$ to determine the mask matrix $\boldsymbol{D}$ for diffusion as follows:

$$\boldsymbol{D} = reshape\left(\left(\mathrm{mod}(r_4 - floor(r_4) \times 2^{32}, 256\right), [h, w]\right) \tag{64}$$

where reshape(.) is to transform the sequence into a matrix.

After determining $\boldsymbol{I}$, $\boldsymbol{T}$, and $\boldsymbol{D}$, each RGB channel of the mixed image $\boldsymbol{M}$ can be encrypted (65), as shown at the bottom of the page, where mod(.) is module operation and the $\oplus$ notation denotes the exclusive *XOR* operation of each bit.

Step 5: Combine three RGB channels of the encrypted $\boldsymbol{E}$ to produce an encrypted image with a size of $(h \times w)$.

b: DECRYPTION

The decrypted algorithm has used the reverse of each step of the proposed encryption algorithm to obtain the original image. Some functions are used to recover the original image hidden in the replacement image as follows:

$$M_{I_{i,j},j} = \begin{cases} \mathrm{mod}\left(D_{i,j} \oplus E_{T_{j,I_{i,j}},I_{i,j}} - M_{T_{h,w},w}, 256\right), & \text{if } i = 1, j = 1 \\ \mathrm{mod}\left(D_{i,j} \oplus E_{I_{i,j},j} - E_{I_{i-1,w},w}, 256\right), & \text{if } i \neq 1, j = 1 \\ \mathrm{mod}\left(D_{i,j} \oplus E_{I_{i,j},j} - E_{I_{i-1,w},w}, 256\right), & \text{if } \forall i, j \neq 1 \end{cases} \tag{66}$$

$$E_{I_{i,j},j} = \begin{cases} mod\left(D_{i,j} \oplus \left(M_{T_{j,I_{i,j}},I_{i,j}} + M_{T_{h,w},w}\right), 256\right), & \text{if } i = 1, j = 1 \\ mod\left(D_{i,j} \oplus \left(M_{T_{j,I_{i,j}},I_{i,j}} + E_{I_{i-1,w},w}\right), 256\right), & \text{if } i \neq 1, j = 1 \\ mod\left(D_{i,j} \oplus \left(M_{T_{j,I_{i,j}},I_{i,j}} + E_{I_{i,j-1},j-1}\right), 256\right), & \text{if } \forall i, j \neq 1 \end{cases} \tag{65}$$

$$\boldsymbol{M} = dct2\,(\boldsymbol{M}) \tag{67}$$
$$\boldsymbol{S} = (\boldsymbol{M} - \boldsymbol{R}) \times \boldsymbol{\rho}^{-1} \tag{68}$$
$$\boldsymbol{S} = idct2\,(\boldsymbol{S}) \tag{69}$$

2) SECURITY ANALYSES

In order to show the efficiency and security of the proposed encryption algorithm, it is used to assess some experimental analyses. Three standard images (Lena, Baboon, and Pepper) using as the main messages and the logo of Yuan Ze University using as the replacement image are applied for security analyses including the histogram and information entropy analyses, correlation coefficients, mean square error (MSE), and peak signal to noise ratio (PSNR), and some attack analyses such as differential attack, noise attack, and cropping attack. The results of these analyses are presented in the following sections.

a: HISTOGRAM

Image histogram describes the distribution of pixel intensity values in the image, and it visually presents the grayscale distribution. The results of color images show that the encrypted image histograms are evenly distributed when compared to the original images (see Figs. 13-15). The mixed images with $\boldsymbol{\rho} = 0.01 \times \boldsymbol{I}_{3\times3}$ including original images and logo image of Yuan Ze University point out that all the original images are hidden, so the image information will be kept as confidential as desired (see Figs. 13-15(b)). The encrypted image and the original image should not have any statistical similarity (see Figs. 13-15(c)). The decrypted images are shown in Figs. 13-15(d). It can be seen that the decrypted images look the same as the original images. In addition, the histograms of original and encrypted images for Lena, Baboon, and Pepper are respectively shown in Figs. 16-18, which clarifies that they are evenly diffused, entirely dissimilar to that for the original image, and there is no statistical similarity to the original image. Hence, the proposed encryption method is resistant to statistical attacks. In addition, this study uses the variances of histograms to test the uniformity of histogram [35], [36]. Variances of histograms is determined as

$$\text{Variance}(\boldsymbol{X}) = \frac{1}{G^2}\sum_{i=1}^{G}\sum_{j=1}^{G}\frac{1}{2}\left(x_i - x_j\right)^2 \tag{70}$$

where $\boldsymbol{X} = [x_1, x_2, \cdots, x_{256}]$ is the vector of the histogram value, x_i and x_j are the numbers of pixels whose gray values are respectively equal to i and j, and G is the greyness level. The lower the variance is, the higher the uniformity of the image obtains. Table 3 shows the histogram variances of Lena for original image and encrypted image that compared with the dynamic DNA encryption and chaos [37], the DNA sequence method [38], and the 3D Brownian motion-based image encryption method [39]. It can be seen that the variance of the encrypted image of our algorithm is less than the values of the variance of [37], [38], and [39]. It implies that the distribution of the histogram of the encrypted image is uniform and the information of the encrypted image can be resistant to statistical attacks.

TABLE 3. Comparison of Average Histogram variances of Lena (512 × 512).

	Original image	Encrypted image
Our method	**950140** (R= 1017300, G= 455720, B= 1377400)	**946.8565** (R= 963.0856, G= 993.8592, B= 883.6248)
Dynamic DNA encryption and chaos method [37]	**950140** (R= 1017300, G= 455720, B= 1377400)	**947.133** (R= 904.758, G= 1013, B= 923.656)
DNA sequence method [38]	**950140** (R= 1017300, G= 455720, B= 1377400)	**1007** (R= 1070, G= 955.320, B= 995.828)
3D Brownian motion-based image encryption method [39]	**950140** (R= 1017300, G= 455720, B= 1377400)	**998.7667** (R= 952.296, G= 1108, B= 935.976)

b: INFORMATION ENTROPY

Information entropy estimates the gray states of an image. If the distribution is uniform, the entropy value can be large, which is calculated by [35]

$$H_E(S) = \sum_{i=0}^{2^Z-1} P_I(S_i) \times \log_2 \frac{1}{P_I(S_i)} \tag{71}$$

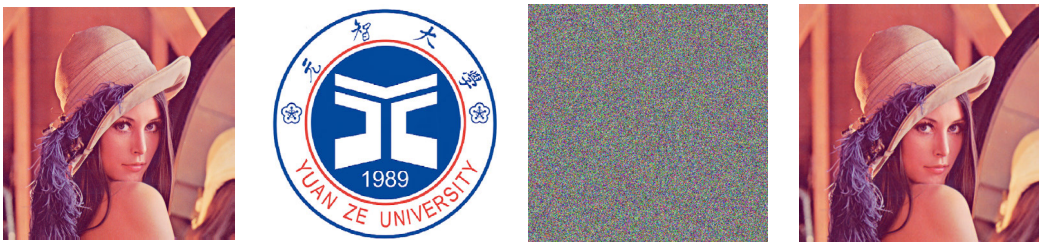
where $P_I(S_i)$ and $H_E(S)$ denote the intensity and entropy values of the encrypted image S. 2^Z is the total states of the data source ($Z = 255$). An actually random image (RI) provides an even distribution of pixel intensities in the range [0, 255], and the entropy value for an ideal RI is 8. Table 4 shows the entropy results, which are computed by different methods such as DNA method [40], hash keying method [41], ciphertext diffusion in crisscross pattern [42], an improved and enhanced method based on hyperchaos [43], DNA encoding method [44], hyper-chaotic and DNA sequences method [45]. It can be observed that their values are approximately 8, so the encrypted image is of maximum randomness leading to the confidentiality of the data. Our method attains greater values than others.

c: CORRELATION BETWEEN TWO NEARBY PIXELS

In this section, we respectively use

pairs of two nearby pixels in three directions (diagonal, horizontal, and vertical) of the original and encrypted images to check the correlation between two nearby pixels of an encrypted image, the below equation can be used [19]:

$$R_{\bar{a}\bar{b}} = \frac{cov(\bar{a}, \bar{b})}{\sqrt{D(\bar{a})}\sqrt{D(\bar{b})}}, \tag{72}$$



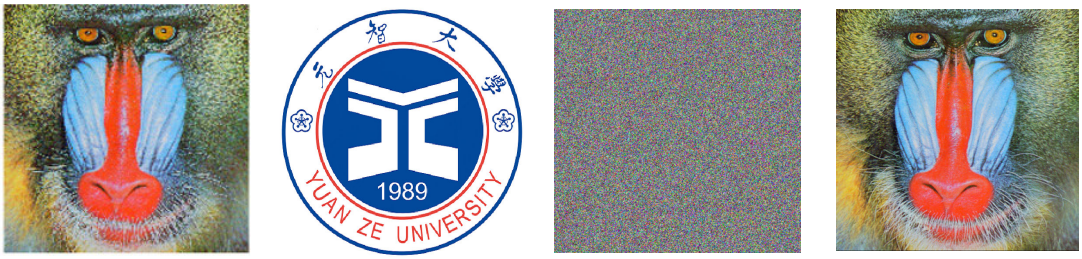
(a) Original image (512×512)

(b) Mixed image with $\rho = 0.01 \times I_{3\times3}$ (including Lena and logo of Yuan Ze University) (512×512)

(c) Encrypted image

(d) Decrypted image

FIGURE 13. Original, mixed, encrypted, and decrypted images of Lena.



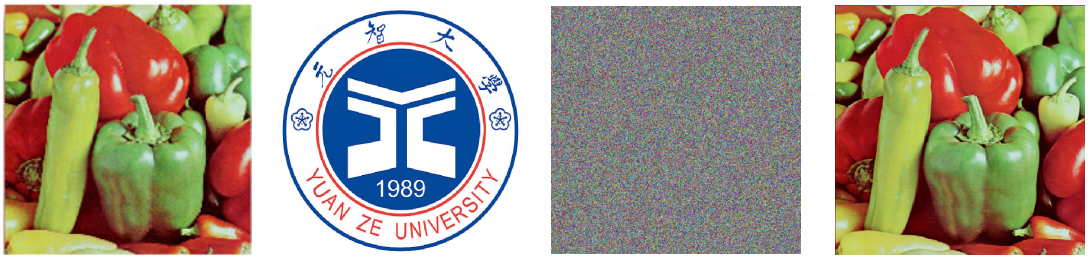
(a) Original image (512×512)

(b) Mixed image with $\rho = 0.01 \times I_{3\times3}$ (including Baboon and logo of Yuan Ze University) (512×512)

(c) Encrypted image

(d) Decrypted image

FIGURE 14. Original, mixed, encrypted, and decrypted images of Baboon.



(a) Original image (512×512)

(b) Mixed image with $\rho = 0.01 \times I_{3\times3}$ (including Peppers and logo of Yuan Ze University) (512×512)

(c) Encrypted image

(d) Decrypted image

FIGURE 15. Original, mixed, encrypted, and decrypted images of Peppers.

where $\bar{a}$ and $\bar{b}$ denote the gray values of two nearby pixels;

$$cov(\bar{a}, \bar{b}) = \frac{1}{Z}\sum_{i=1}^{Z}(\bar{a}_i - E(\bar{a}))\left(\bar{b}_i - E(\bar{b})\right),$$

$$E(\bar{a}) = \frac{1}{Z}\sum_{i=1}^{Z}\bar{a}_i; \quad D(\bar{a}) = \frac{1}{Z}\sum_{i=1}^{Z}(\bar{a}_i - E(\bar{a}))^2,$$

$$E(\bar{b}) = \frac{1}{Z}\sum_{i=1}^{Z}\bar{b}_i \text{ and } D(\bar{b}) = \frac{1}{Z}\sum_{i=1}^{Z}\left(\bar{b}_i - E(\bar{b})\right)^2.$$

The correlation distributions between the encrypted and original images for Lena, baboon, and peppers are respectively shown in Figs. 19-21. Our method efficiently reduces the correlation of pixels compared to DNA method [40], ciphertext diffusion in crisscross pattern [42], an improved and enhanced method based on hyperchaos [43], DNA encoding method [44], and hyperchaotic and DNA sequences method [45]. The correlation coefficients between two nearby pixels of the original images are calculated in Table 5, which shows that two nearby pixels of the original images are completely different. The correlation coefficients between

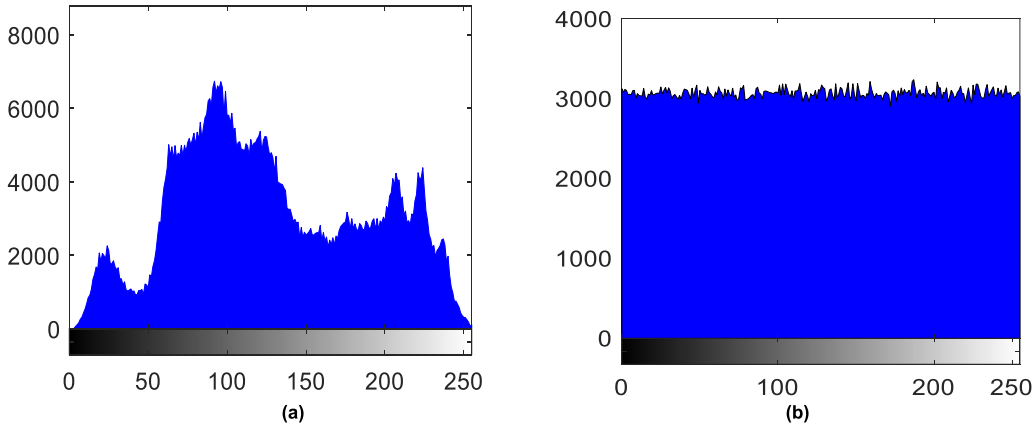


FIGURE 16. Histogram of Lena (a) original image and (b) encrypted image.

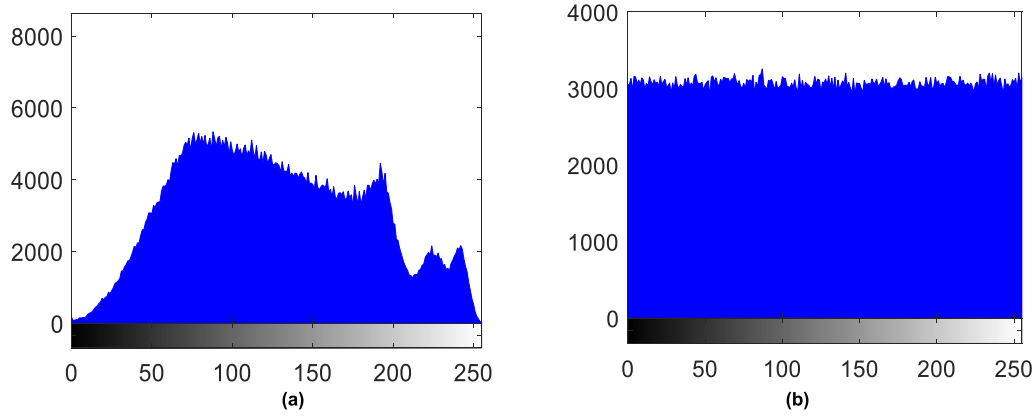


FIGURE 17. Histogram of Baboon (a) original image and (b) encrypted image.

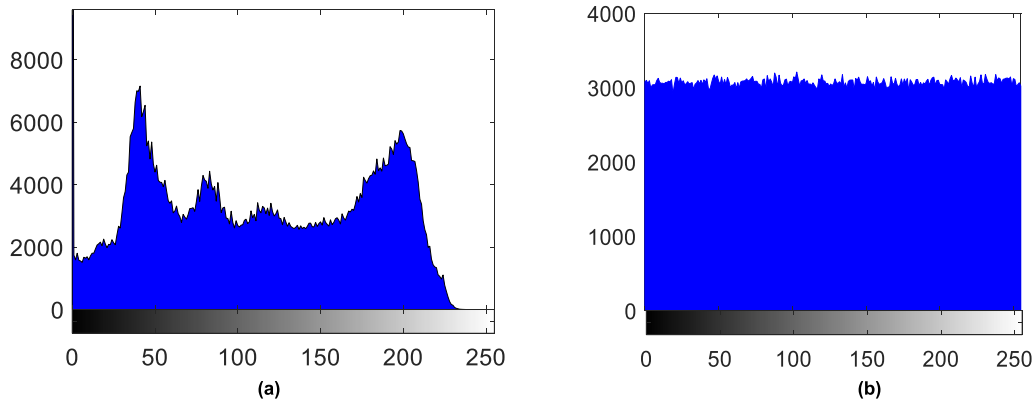


FIGURE 18. Histogram of Peppers (a) original image and (b) encrypted image.

two nearby pixels of the encrypted images is remarkably decreased and roughly 0 in the encrypted images (see Table 6), it indicates that two nearby pixels of the encrypted images are quite the same. This further demonstrates that our method can efficiently oppose statistical attacks.

d: MEAN SQUARE ERROR (MSE) AND PEAK SIGNAL-TO-NOISE RATIO (PSNR)

Through histogram analysis, there is a significant difference in the pixel distribution of the encrypted image. But for more accurate evaluations of the proposed encryption

TABLE 4. Entropy analysis of the images.

	Encrypted image						
	Our method	DNA method [40]	Hash keying method [41]	Ciphertext diffusion in crisscross pattern [42]	An improved and enhanced method based on hyperchaos [43]	DNA encoding method [44]	Hyper-chaotic and DNA sequences method [45]
Lena	7.9998	7.9984	7.9976	7.9968	7.9970	7.9974	7.9964
Peppers	7.9998	7.9984	--	7.9993	7.9993	7.9993	7.9992
Baboon	7.9998	7.9985	--	--	--	--	--

TABLE 5. Correlation coefficients between two nearby pixels of the original images.

	Original images		
	Horizontal	*Vertical*	*Diagonal*
Lena	0.9719	0.9850	0.9593
Baboon	0.9850	0.7587	0.7262
Peppers	0.9768	0.9792	0.9639

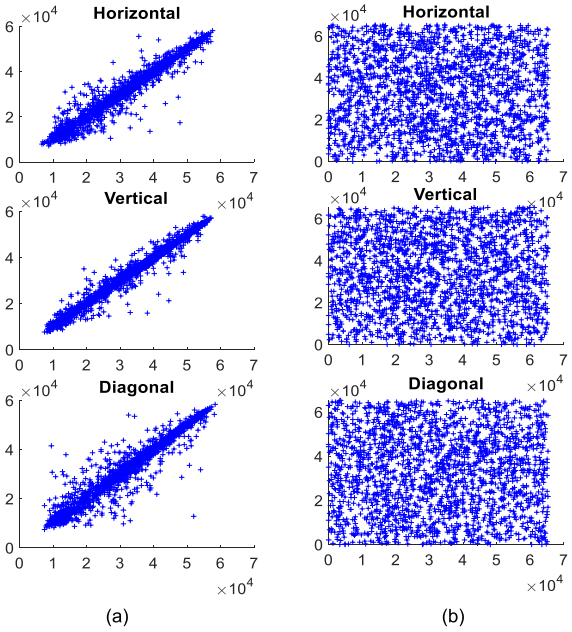


FIGURE 19. Correlations of two nearby pixels of Lena (a) original images and (b) encrypted images.

algorithm, the differences between the original and encrypted images have been calculated. The MSE is determined by (67) [41], [47]. The larger the MSE, the better security of the method is obtained. In addition, the similarity measurement index that is the PSNR is applied for measuring the distances between pixels. The PSNR of the original and encrypted images is given as in (68) [41], [47].

$$\text{MSE} = \frac{1}{(N \times M)} \sum_{i=1}^{N} \sum_{j=1}^{M} [o(i,j) - e(i,j)]^2 \quad (73)$$

$$\text{PSNR} = 10 \times log_{10} \left(\frac{I_{Max}^2}{\text{MSE}} \right) \text{(db)} \quad (74)$$

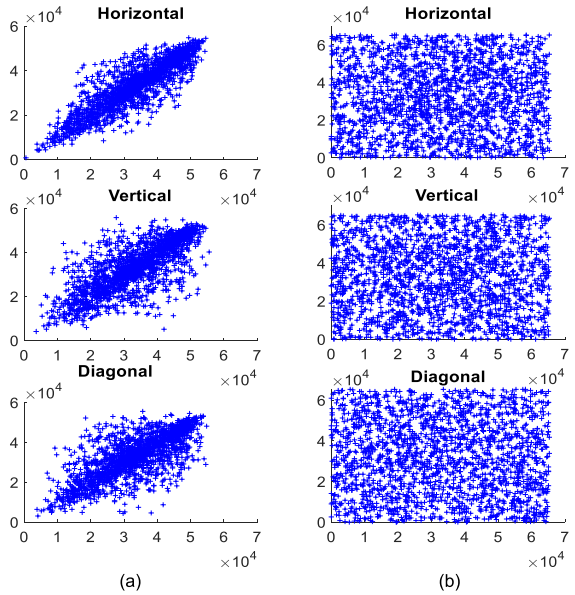


FIGURE 20. Correlations of two nearby pixels of Baboon (a) original images and (b) encrypted images.

where $(N \times M)$ is the number of pixels in the image. $I_{Max} = 255$ is the maximum pixel value of the encrypted image. And $o(i, j)$ and $e(i, j)$ are respectively the pixel gray value of the original and encrypted images at a location (i, j).

MSE for the original and encrypted images using the proposed scheme is shown in Table 7. The PSNR between the proposed method and the former methods is presented in Table 8. Analysis results indicate that our method achieves better performance and quality than DNA method [40] and robust and lossless color image encryption method [46].

e: DIFFERENTIAL ATTACK ANALYSIS

This study uses number of pixels change rate (NPCR) and unified average changing intensity (UACI) to test the resisting differential attack performance of the proposed encryption method. For the original image I, randomly change one bit in I to obtain I'. D and D' are respectively the encrypted images of I and I'. The values of NPCR and UACI of red, green and blue components of the encrypted image can be calculated by [37]

$$NPCR = \frac{\sum_{i,j} \Delta D\,(i,j)}{N \times M} \times 100\% \quad (75)$$

TABLE 6. Correlation coefficients between two nearby pixels of the encrypted images using different methods.

		Encrypted image					
		Our method	DNA method [40]	Ciphertext diffusion in crisscross pattern [42]	An improved and enhanced method based on hyperchaos [43]	DNA encoding method [44]	Hyper-chaotic and DNA sequences method [45]
Lena	Horizontal	0.0005	--	-0.0021	-0.0043	-0.0047	0.0019
	Vertical	0.0002	--	-0.0042	-0.0034	0.0040	-0.0030
	Diagonal	-0.00005	--	-0.0022	0.0041	-0.0034	0.0018
Peppers	Horizontal	0.0005	--	-0.0015	-0.0019	-0.0025	0.0009
	Vertical	-0.00001	--	-0.0012	0.0018	-0.0025	0.0041
	Diagonal	0.0006	--	0.0017	0.0002	0.0013	0.0008
Baboon	Horizontal	0.00004	-0.0357	--	--	--	--
	Vertical	-0.0009	-0.0223	--	--	--	--
	Diagonal	0.0008	-0.0223	--	--	--	--

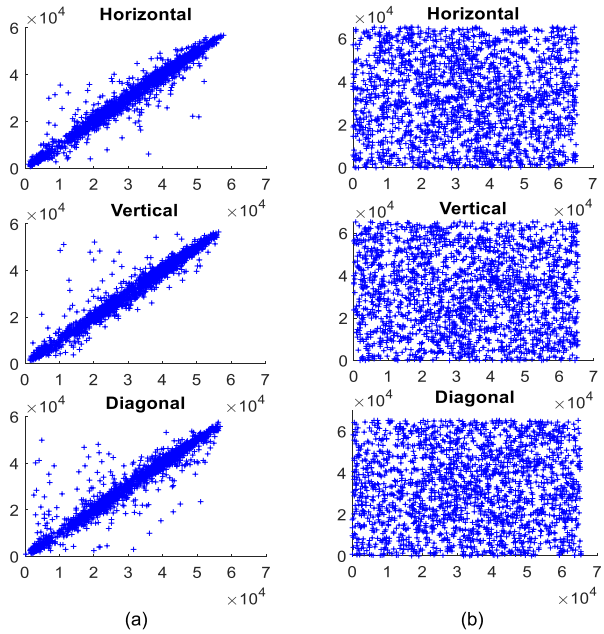


FIGURE 21. Correlations of two nearby pixels of Peppers (a) original images and (b) encrypted images.

$$UACI = \frac{1}{N \times M}\left[\sum_{i,j}\frac{D'(i,j) - D(i,j)}{255}\right] \times 100\% \quad (76)$$

where $\Delta D(i,j)$ is

$$\Delta D(i,j) = \begin{cases} 1, & D'(i,j) \neq D(i,j) \\ 0, & D'(i,j) = D(i,j) \end{cases} \quad (77)$$

where N and M are respectively the width and height of the image.

For instance, for two random images, the expected values of NPCR and UACI for an 8 bit grey image are NPCR = 99.6094% and UACI = 33.4635%. [37]. The NPCR and UACI results for Lena, Peppers and Baboon images are respectively shown in Table 9 and 10. Moreover, average performance of NPCR and UACI are respectively shown in Table 11 and 12. The results show that changing a pixel value in an image can lead to a high resistance value. The respective results of NPCR and UACI are 99.6% and 33.4% showing that our method is able to resist attacks.

TABLE 7. MSE between the original and encrypted images for our method.

Images	MSE
Lena	1.4903 x 10^4
Baboon	1.4880 x 10^4
Peppers	1.4910 x 10^4

f: NOISE ATTACK ANALYSIS

In reality, images are attacked by noise during communication, and using the encrypted image is a defense against that attack. In this section, the Lena image is used as a test image for the proposed method. Fig. 22 depicts the encrypted image with noise Gaussian noise (GN), Salt & Pepper noise (SPN), and Speckle noise (SN) with different noise densities and their decrypted images. As seen from Fig. 22, almost all information of the original image has been successfully decrypted.

As seen in Table 13, the proposed method obtains good resistance, where the average PSNR for speckle noise is larger than 32 dB, the average PSNR for Gaussian noise is larger than 28 dB, and the average PSNR for salt & pepper noise is larger than 24 dB.

g: CROPPING ATTACK ANALYSIS

Similar to noise attack analysis, the proposed method is also successful against data loss. Fig. 23 depicts the encrypted images with different lost data impacts and their corresponding recovered images. Also, Table 14 shows the quantitative results of cropping attacks. As seen in Fig. 23 and Table 14, the recovery images can be recognized even though the encrypted images have lost 6.25 % to 25% of their information and the PSNR value is approximately 11 dB to 27 dB. Obviously, the decrypted images still restore most data of the original image.

h: NIST SP800-22 TEST RESULTS

The National Institute of Standards and Technology (NIST) SP800-22 index [47] is used to test the randomness of the

TABLE 8. PSNR of the encrypted images for different methods.

Images	PSNR (original-encrypted images)			PSNR (original-decrypted images)		
	Our method	DNA method [40]	Robust and lossless color image encryption method [46]	Our method	DNA method [40]	Robust and lossless color image encryption method [46]
Lena	6.3980	8.7084	8.1293	∞	∞	∞
Baboon	6.4048	9.0996	8.7729	∞	∞	∞
Peppers	6.3959	8.2003	7.6393	∞	∞	∞

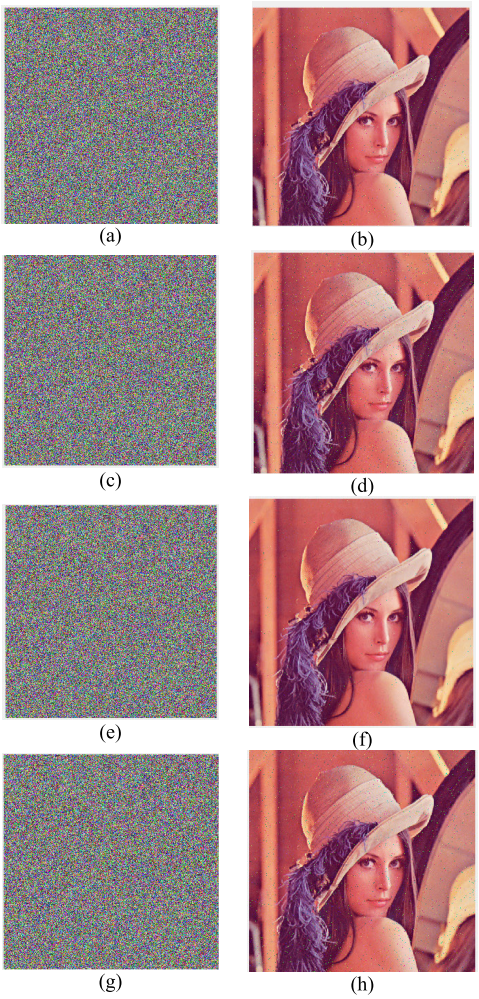


FIGURE 22. Noise attack results. (a) Noisy images by salt & pepper with density = 0.002, (b) decrypted image of (a); (c) Noisy images by salt & pepper with density = 0.005, (d) decrypted image of (c); (e) Noisy images by speckle with density = 0.000002, (f) decrypted image of (e); (g) Noisy images by Gaussian with density = 0.000001, and (h) decrypted image of (g).

TABLE 9. NPCR results for Lena, Baboon and Peppers.

	NPCR	NPCR Critical values		
		$N^*_{0.05}$	$N^*_{0.01}$	$N^*_{0.001}$
Lena	0.9962	Pass	Pass	Pass
Peppers	0.9961	Pass	Pass	Pass
Baboon	0.9962	Pass	Pass	Pass

output sequences. The NIST SP800-22 has 15 sub-tests and a *P*-value may be generated by every sub-test. Based on the instruction of [47], 100 bits in 262144 (512 × 512) bits of encrypted image are used as input data and the corresponding *P*-value is expected to fall into the range of 0.01 and 1 to pass the test. Table 15 lists the test results. It is clear that the binary streams of the encrypted image can pass all the sub-tests. Therefore, the randomness of the pixels of the encrypted image is confirmed.

TABLE 10. UACI results for Lena, Baboon and Peppers.

	UACI (%)	UACI Critical values		
		$N^*_{0.05}$	$N^*_{0.01}$	$N^*_{0.001}$
Lena	33.47	Pass	Pass	Pass
Peppers	33.48	Pass	Pass	Pass
Baboon	33.48	Pass	Pass	Pass

TABLE 11. Average performance of NPCR.

	Lena	Peppers	Baboon
Ciphertext diffusion in crisscross pattern [42]	1	0.9966	0.9964
An improved and enhanced method based on hyperchaos [43]	0.9966	0.9956	0.9955
Hyper-chaotic and DNA sequences method [45]	0.5974	0.5380	0.5378
Dynamic DNA encryption and chaos [37]	0.9961	--	--
DNA sequence [38]	0.9959	--	0.9961
Our method	0.9962	0.9961	0.9962

TABLE 12. Average performance of UACI(%).

	Lena	Peppers	Baboon
Ciphertext diffusion in crisscross pattern [42]	33.5752	33.5030	33.5237
An improved and enhanced method based on hyperchaos [43]	33.4263	33.44255	33.44255
Hyper-chaotic and DNA sequences method [45]	25.0487	22.2575	22.2575
Dynamic DNA encryption and chaos [37]	33.50	--	--
DNA sequence [38]	33.45	--	33.43
Our method	33.47	33.48	33.48

TABLE 13. Quantitative results of resisting noise attacks.

		Average of PSNR (original-decrypted images) (dB)	
Density	Type of resisting noise	Our method	Dynamic DNA encryption and chaos [36]
0.002	Salt & pepper	28.7975	34.4133
0.005	Salt & pepper	24.8322	31.0500
0.000002	Speckle	32.9263	26.9833
0.000001	Gaussian	28.8625	24.2800

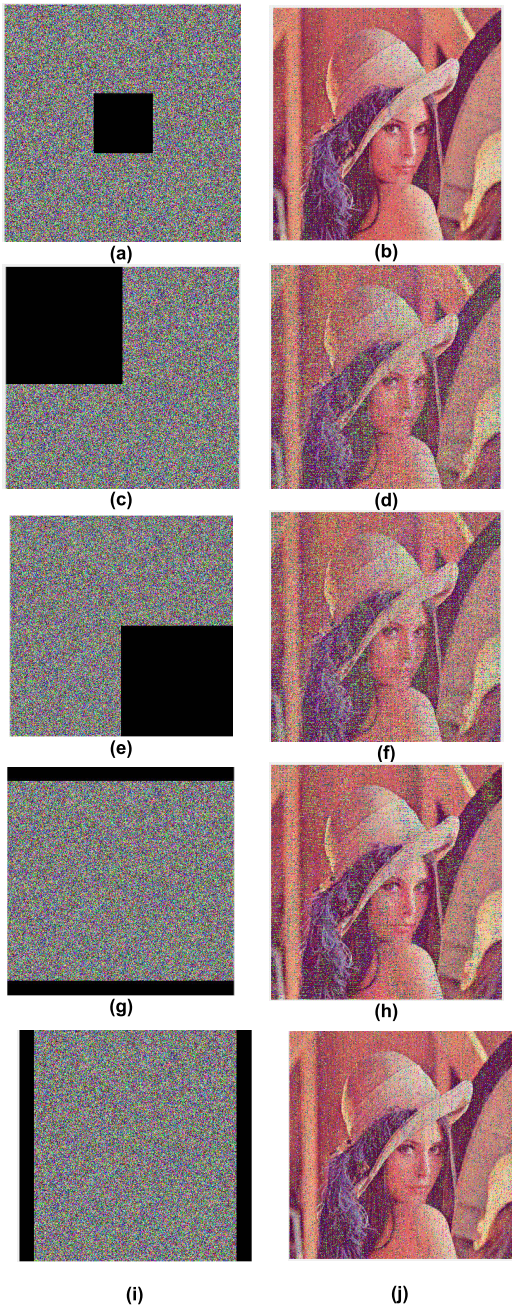


FIGURE 23. Quantitative results of cropping attacks (a) Encrypted image with 1/16 data loss at the center, (c) Encrypted image with 1/4 data loss at the top-left corner, (e) Encrypted image with 1/4 data loss at the bottom-right corner, (g) Encrypted image with 1/16 data loss the top side and 1/16 data loss at the bottom side, (i) Encrypted image with 1/16 data loss the left side and 1/16 data loss at the right side, (b), (d), (f), (h), (j) are decrypted images of (a), (c), (e), (g) and (i), respectively.

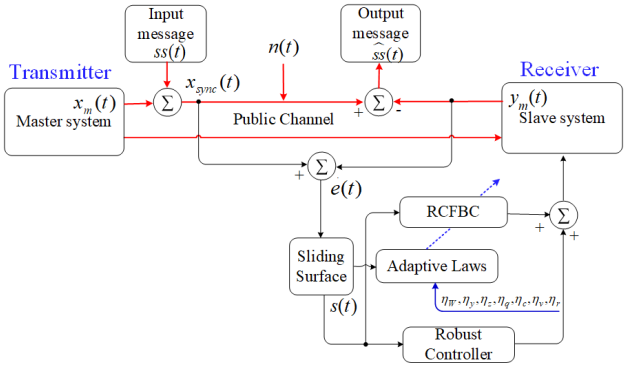


FIGURE 24. The structure of the audio secure communication using chaotic synchronization, $x_m(t)$ is master signal, $ss(t)$ is source signal, $x_{sync}(t)$ synchronized signal, $n(t)$ is noise signal, $y_m(t)$ is slave signal, $\hat{ss}(t)$ is received audio signal.

TABLE 14. Quantitative results of cropping attacks.

	Average of PSNR (original-decrypted images) (dB)	
	Our method	Hyper-chaotic and DNA sequences method [45]
1/16 data loss at the center	27.95	24.13
1/4 data loss at the top-left corner	11.19	--
1/4 data loss at the bottom-right corner	12.06	--
1/16 the top side and 1/16 the bottom side	13.36	12.21
1/16 the right side and 1/16 the left side	15.40	12.35

TABLE 15. NIST test results for encrypted image.

	Statistical test	P value ≥ 0.01	Results
1	Frequency	0.5271	Pass
2	Discrete Fourier transform	0.1225	Pass
3	Approximate Entropy	0.5632	Pass
4	Cumulative sums forward	0.0578	Pass
5	Cumulative sums reserve	0.0625	Pass
6	Linear complexity	0.1217	Pass
7	Longest run	0.0852	Pass
8	Overlapping templates	0.2114	Pass
9	Random-excursions	0.1213	Pass
10	Random-excursions variant	0.1204	Pass
11	Rank	0.3854	Pass
12	Runs	0.2661	Pass
13	Serial p-value 1	0.1215	Pass
14	Serial p-value 2	0.3321	pass
15	Universal	0.5484	Pass

C. SECURE COMMUNICATION FOR AUDIO SIGNAL USING 3D GENESIO CHAOTIC SYNCHRONIZATION

The proposed RCFBC synchronization scheme is also used for audio secure communications. Fig. 24 shows the proposed structure of audio secure communication including a transmitter (master system $x_m(t)$) and a receiver (slave system $y_m(t)$). The input audio signal $ss(t)$ is masked by a state of the master chaotic system, which is concurrently transmitted to the receiver. Moreover, the output signal is sent to the receiver for synchronization using the proposed control system. It is assumed that there has a white Gaussian noise $n(t)$ on the public channel. Finally, the synchronization between the transmitter and the receiver can be attained, and the output audio signal $\hat{ss}(t)$ is completely restored on the receiver.

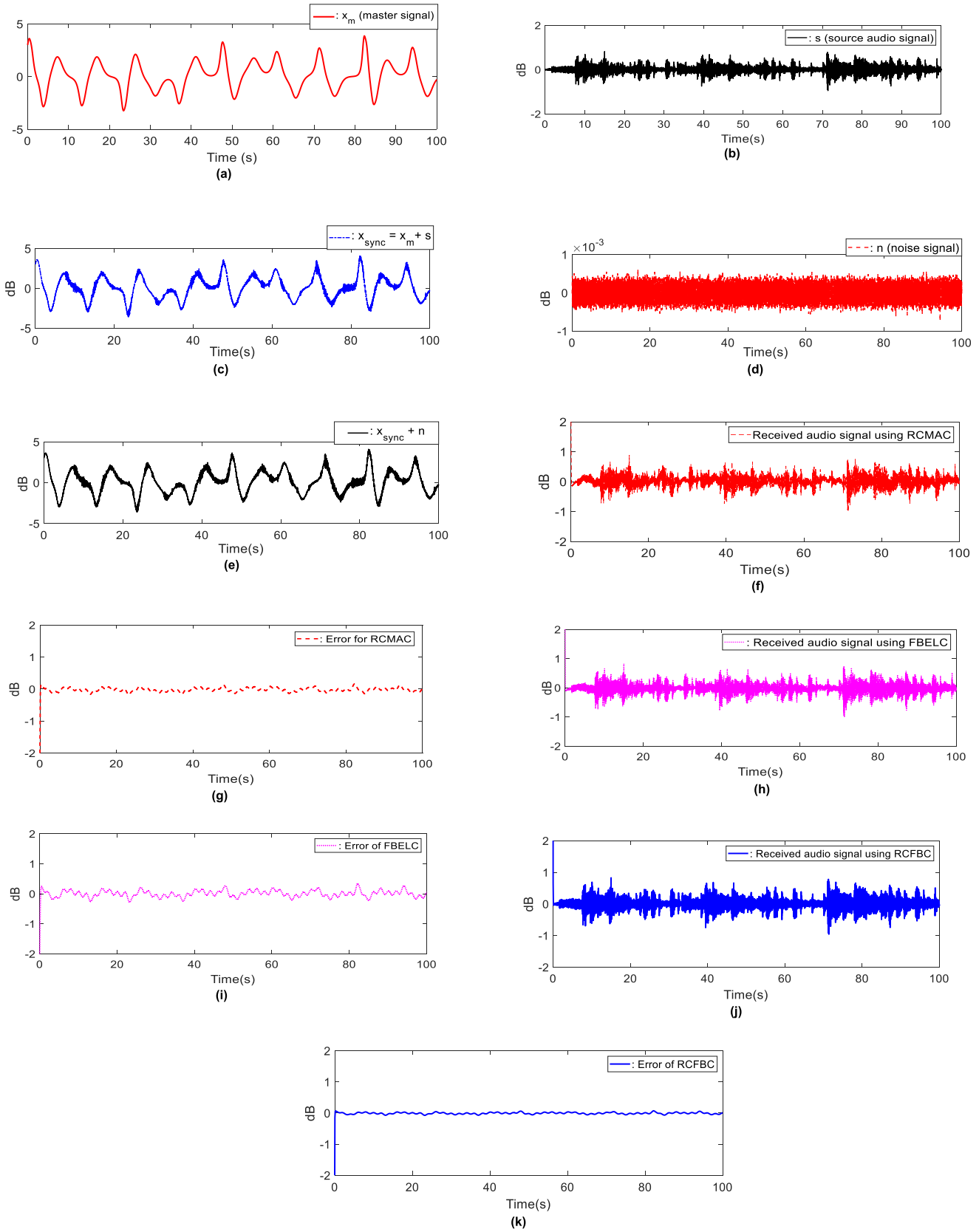


FIGURE 25. The simulation results of the audio secure communication using chaotic synchronization. (a) Master signal, (b) source audio signal, (c) masked audio signal, (d) noise signal, (e) masked audio signal adding noise, (f) audio received signal using RCMAC, (g) error using RCMAC, (h) audio received signal using FBELC, (i) error using FBELC, (j) audio received signal using RCFBC, (k) error using RCFBC.

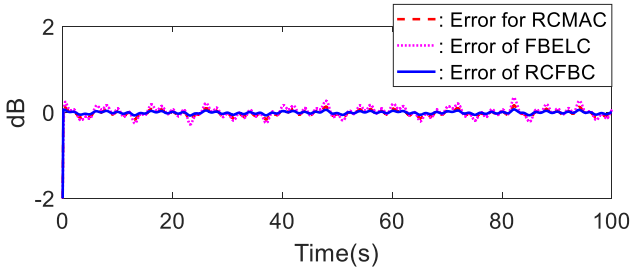


FIGURE 26. Errors for audio secure communication in chaotic synchronization.

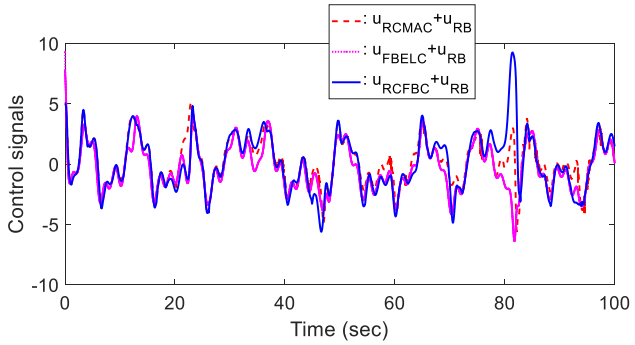


FIGURE 27. Control signals for audio secure communication in chaotic synchronization.

TABLE 16. Comparison in RMSE for different methods.

Method	RMSE
RCMAC [34]	0.0423
FBELC [11]	0.0411
T2FBELC [13]	0.0325
WIT2FQFLBEC [31]	0.0279
RCFBC	0.0164

Figure 25 (a)–(k) shows the simulation results for the audio secure communication using chaotic synchronization between state $x_m(t)$ and state $y_m(t)$, in which Fig. 23 (c) shows the masked audio signal by $x_m(t)$. It can be observed that the masked signal becomes more chaotic than the original signal. Therefore, restoring the original signal from the transmitted signal is not easy without synchronization between the receiver and transmitter. Fig. 25 (e) shows the masked audio signal adding noise on the public channel. Fig. 25 (f), (h), and (j) show the recovered audio signal that can be fully restored on the receiver by using the RCMAC [34], FBELC [11], T2FBELC [13], WIT2FQFLBEC [31], and the proposed RCFBC, respectively. Figs. 26 and 27 show the errors and control signals for audio secure communication in chaotic synchronization. In addition, a comparison in RMSE for different methods is given in Table 8. The simulation results show that audio secure communication is achieved by using the proposed method. The proposed RCFBC system gives better performance than the others.

TABLE 17. NIST test results for genesio chaotic.

	Statistical test	P value ≥ 0.01	Results
1	Frequency	0.0578	Pass
2	Discrete Fourier transform	0.2250	Pass
3	Approximate Entropy	0.2411	Pass
4	Cumulative sums forward	0.0235	Pass
5	Cumulative sums reserve	0.0125	Pass
6	Linear complexity	0.2256	Pass
7	Longest run	0.0244	Pass
8	Overlapping templates	0.6125	Pass
9	Random-excursions	0.3005	Pass
10	Random-excursions variant	0.0423	Pass
11	Rank	0.4276	Pass
12	Runs	0.1256	Pass
13	Serial p-value 1	0.1729	Pass
14	Serial p-value 2	0.2318	Pass
15	Universal	0.3356	Pass

VI. CONCLUSION

This paper presents the synchronization of the 3D Genesio chaotic system and its applications for secure communication of images and audio signals. The parameter adaptive laws are developed by the architecture of human brain nervous systems, and the Lyapunov stability theorem is used to guarantee the convergence and system stability. The proposed control algorithm is applied to efficiently synchronize the master and slave systems. In addition, an image encryption-decryption algorithm is proposed for image secure communication, and the cryptanalysis shows that the efficiency and security of the proposed encryption algorithm can be achieved. In summary, the proposed method is an efficient scheme for safe image and audio signal transmissions in real-world communication applications. Firstly, future work can combine the proposed encrypted algorithm with a watermarking algorithm to provide a secure transfer and with the secret key for various applications such as video, audio, and image communications.

APPENDIX

In this study, the use of the Genesio chaotic system has to satisfy the test results listed in Table 17, in which all P-value of 15 sub-tests must be larger or equal to 0.01 to pass the NIST (National Institute of Standards and Technology SP800-22) test. It can be seen that the binary streams of the Genesio chaotic system have passed all the sub-tests, which means that the Genesio chaotic system is quite suitable for image encryption.

REFERENCES

[1] Y. Yu and S. Zhang, "Adaptive backstepping synchronization of uncertain chaotic system," *Chaos, Solitons Fractals*, vol. 21, no. 3, pp. 643–649, Jul. 2004.
[2] J. H. Park, "Adaptive synchronization of Rossler system with uncertain parameters," *Chaos, Solitons Fractals*, vol. 25, no. 2, pp. 333–338, Jul. 2005.
[3] Y.-F. Peng and C.-F. Hsu, "Identification-based chaos control via backstepping design using self-organizing fuzzy neural networks," *Chaos, Solitons Fractals*, vol. 41, no. 3, pp. 1377–1389, Aug. 2009.

[4] M. P. Aghababa and A. Heydari, "Chaos synchronization between two different chaotic systems with uncertainties, external disturbances, unknown parameters and input nonlinearities," *Appl. Math. Model.*, vol. 36, no. 4, pp. 1639–1652, Apr. 2012.

[5] A. T. Azar and S. Vaidyanathan, *Advances in Chaos Theory and Intelligent Control*. Cham, Switzerland: Springer, 2016.

[6] J. Sun, Y. Shen, Q. Yin, and C. Xu, "Compound synchronization of four memristor chaotic oscillator systems and secure communication," *Chaos, Interdiscipl. J. Nonlinear Sci.*, vol. 23, no. 1, Mar. 2013, Art. no. 013140.

[7] Q. Wang, Q. Zhang, and X. Wei, "Image encryption algorithm based on DNA biological properties and chaotic systems," in *Proc. IEEE 5th Int. Conf. Bio-Inspired Comput., Theories Appl. (BIC-TA)*, Sep. 2010, pp. 132–136.

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

[9] M. H. Al Hasani and K. A. Al Naimee, "Impact security enhancement in chaotic quantum cryptography," *Opt. Laser Technol.*, vol. 119, Nov. 2019, Art. no. 105575.

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

[11] C.-M. Lin and C.-C. Chung, "Fuzzy brain emotional learning control system design for nonlinear systems," *Int. J. Fuzzy Syst.*, vol. 17, no. 2, pp. 117–128, Jun. 2015.

[12] D. Zhou, F. Chao, C.-M. Lin, L. Yang, M. Shi, and C. Zhou, "Integration of fuzzy CMAC and BELC networks for uncertain nonlinear system control," in *Proc. IEEE Int. Conf. Fuzzy Syst. (FUZZ-IEEE)*, Jul. 2017, pp. 1–6.

[13] T.-L. Le, C.-M. Lin, and T.-T. Huynh, "Self-evolving type-2 fuzzy brain emotional learning control design for chaotic systems using PSO," *Appl. Soft Comput.*, vol. 73, pp. 418–433, Dec. 2018.

[14] T.-T. Huynh and C.-M. Lin, "Wavelet dual function-link fuzzy brain emotional learning system design for system identification and trajectory tracking of nonlinear systems," in *Proc. IEEE Int. Conf. Syst., Man Cybern. (SMC)*, Oct. 2019, pp. 1653–1657.

[15] T.-T. Huynh, C.-M. Lin, T.-T.-T. Pham, H.-Y. Cho, and T.-L. Le, "A modified function-link fuzzy cerebellar model articulation controller using a PI-type learning algorithm for nonlinear system synchronization and control," *Chaos, Solitons Fractals*, vol. 118, pp. 65–82, Jan. 2019.

[16] H. Liu, A. Kadir, and Y. Li, "Audio encryption scheme by confusion and diffusion based on multi-scroll chaotic system and one-time keys," *Optik*, vol. 127, no. 19, pp. 7431–7438, 2016.

[17] J. B. Lima and E. F. da Silva Neto, "Audio encryption based on the cosine number transform," *Multimedia Tools Appl.*, vol. 75, no. 14, pp. 8403–8418, Jul. 2016.

[18] P. Sathiyamurthi and S. Ramakrishnan, "Speech encryption using chaotic shift keying for secured speech communication," *EURASIP J. Audio, Speech, Music Process.*, vol. 2017, no. 1, pp. 1–11, Dec. 2017.

[19] L. Shanmugam, P. Mani, R. Rajan, and Y. H. Joo, "Adaptive synchronization of reaction–diffusion neural networks and its application to secure communication," *IEEE Trans. Cybern.*, vol. 50, no. 3, pp. 911–922, Mar. 2020.

[20] G. Xu, Y. Shekofteh, A. Akgül, C. Li, and S. Panahi, "A new chaotic system with a self-excited attractor: Entropy measurement, signal encryption, and parameter estimation," *Entropy*, vol. 20, no. 2, p. 86, Jan. 2018.

[21] D. Chang, Z. Li, M. Wang, and Y. Zeng, "A novel digital programmable multi-scroll chaotic system and its application in FPGA-based audio secure communication," *AEU-Int. J. Electron. Commun.*, vol. 88, pp. 20–29, May 2018.

[22] Z. Man, J. Li, X. Di, and O. Bai, "An image segmentation encryption algorithm based on hybrid chaotic system," *IEEE Access*, vol. 7, pp. 103047–103058, 2019.

[23] M. Kalpana, K. Ratnavelu, and P. Balasubramaniam, "An audio encryption based on synchronization of robust BAM FCNNs with time delays," *Multimedia Tools Appl.*, vol. 78, no. 5, pp. 5969–5988, Mar. 2019.

[24] F. Yang, J. Mou, Y. Cao, and R. Chu, "An image encryption algorithm based on BP neural network and hyperchaotic system," *China Commun.*, vol. 17, no. 5, pp. 21–28, May 2020.

[25] R. I. Abdelfatah, "Audio encryption scheme using self-adaptive bit scrambling and two multi chaotic-based dynamic DNA computations," *IEEE Access*, vol. 8, pp. 69894–69907, 2020.

[26] M. Samimi, M. H. Majidi, and S. Khorashadizadeh, "Secure communication based on chaos synchronization using brain emotional learning," *AEU-Int. J. Electron. Commun.*, vol. 127, Dec. 2020, Art. no. 153424.

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

[28] Z.-H. Guan, F. Huang, and W. Guan, "Chaos-based image encryption algorithm," *Phys. Lett. A*, vol. 346, nos. 1–3, pp. 153–157, Oct. 2005.

[29] C. Çokal and E. Solak, "Cryptanalysis of a chaos-based image encryption algorithm," *Phys. Lett. A*, vol. 373, no. 15, pp. 1357–1360, Mar. 2009.

[30] T.-T. Huynh, C.-M. Lin, T.-L. Le, H.-Y. Cho, T.-T.-T. Pham, N.-Q.-K. Le, and F. Chao, "A new self-organizing fuzzy cerebellar model articulation controller for uncertain nonlinear systems using overlapped Gaussian membership functions," *IEEE Trans. Ind. Electron.*, vol. 67, no. 11, pp. 9671–9682, Nov. 2020.

[31] T.-T. Huynh, C.-M. Lin, T.-L. Le, N. P. Nguyen, S.-K. Hong, and F. Chao, "Wavelet interval type-2 fuzzy quad-function-link brain emotional control algorithm for the synchronization of 3D nonlinear chaotic systems," *Int. J. Fuzzy Syst.*, vol. 22, no. 8, pp. 2546–2564, Nov. 2020.

[32] C.-M. Lin, Y.-F. Peng, and M.-H. Lin, "CMAC-based adaptive backstepping synchronization of uncertain chaotic systems," *Chaos, Solitons Fractals*, vol. 42, no. 2, pp. 981–988, Oct. 2009.

[33] C.-M. Lin, T.-T. Huynh, and T.-L. Le, "Adaptive TOPSIS fuzzy CMAC back-stepping control system design for nonlinear systems," *Soft Comput.*, vol. 23, no. 16, pp. 6947–6966, Aug. 2019.

[34] R.-J. Wai, C.-M. Lin, and Y.-F. Peng, "Adaptive hybrid control for linear piezoelectric ceramic motor drive using diagonal recurrent CMAC network," *IEEE Trans. Neural Netw.*, vol. 15, no. 6, pp. 1491–1506, Nov. 2004.

[35] Y. Xu, H. Wang, Y. Li, and B. Pei, "Image encryption based on synchronization of fractional chaotic systems," *Commun. Nonlinear Sci. Numer. Simul.*, vol. 19, no. 10, pp. 3735–3744, Oct. 2014.

[36] T. Li, J. Shi, and D. Zhang, "Color image encryption based on joint permutation and diffusion," *J. Electron. Imag.*, vol. 30, no. 1, Feb. 2021, Art. no. 013008.

[37] X. Chai, Y. Chen, and L. Broyde, "A novel chaos-based image encryption algorithm using DNA sequence operations," *Opt. Lasers Eng.*, vol. 88, pp. 197–213, Jan. 2017.

[38] X. Chai, X. Fu, Z. Gan, Y. Lu, and Y. Chen, "A color image cryptosystem based on dynamic DNA encryption and chaos," *Signal Process.*, vol. 155, pp. 44–62, Feb. 2019.

[39] Z. Gan, X. Chai, M. Zhang, and Y. Lu, "A double color image encryption scheme based on three-dimensional brownian motion," *Multimedia Tools Appl.*, vol. 77, no. 21, pp. 27919–27953, Nov. 2018.

[40] M. Samiullah, W. Aslam, H. Nazir, M. I. Lali, B. Shahzad, M. R. Mufti, and H. Afzal, "An image encryption scheme based on DNA computing and multiple chaotic systems," *IEEE Access*, vol. 8, pp. 25650–25663, 2020.

[41] T. Gopalakrishnan and S. Ramakrishnan, "Chaotic image encryption with hash keying as key generator," *IETE J. Res.*, vol. 63, no. 2, pp. 172–187, Mar. 2017.

[42] C.-X. Zhu, Y.-P. Hu, and K.-H. Sun, "New image encryption algorithm based on hyperchaotic system and ciphertext diffusion in crisscross pattern," *Dianzi Yu Xinxi Xuebao, J. Electron. Inf. Technol.*, vol. 34, no. 7, pp. 1735–1743, 2012.

[43] Z. Cong-Xu and S. Ke-Hui, "Cryptanalysis and improvement of a class of hyperchaos based image encryption algorithms," *Acta Phys. Sinica*, vol. 61, no. 12, 2012, Art. no. 120503.

[44] X. Wang and C. Liu, "A novel and effective image encryption algorithm based on chaos and DNA encoding," *Multimedia Tools Appl.*, vol. 76, no. 5, pp. 6229–6245, Mar. 2017.

[45] K. Zhan, D. Wei, J. Shi, and J. Yu, "Cross-utilizing hyperchaotic and DNA sequences for image encryption," *J. Electron. Imag.*, vol. 26, no. 1, Feb. 2017, Art. no. 013021.

[46] X. Wu, J. Kurths, and H. Kan, "A robust and lossless DNA encryption scheme for color images," *Multimedia Tools Appl.*, vol. 77, no. 10, pp. 12349–12376, May 2018.

[47] L. Bassham, A. Rukhin, J. Soto, J. Nechvatal, M. Smid, E. Barker, S. Leigh, M. Levenson, M. Vangel, D. Banks, A. Heckert, J. Dray, and S. Vo, "A statistical test suite for random and pseudorandom number generators for cryptographic applications," Nat. Inst. Standards Technol., Gaithersburg, MD, USA, Tech. Rep. SP-800-22 Rev. 1a, 2010.

CHIH-MIN LIN (Fellow, IEEE) was born in Changhua, Taiwan, in 1959. He received the B.S. and M.S. degrees from the Department of Control Engineering, National Chiao Tung University, Hsinchu, Taiwan, in 1981 and 1983, respectively, and the Ph.D. degree from the Institute of Electronics Engineering, National Chiao Tung University, in 1986. From 1997 to 1998, he was the Honor Research Fellow with The University of Auckland, New Zealand. He is currently a Chair Professor and the Vice President of Yuan Ze University, Taoyuan, Taiwan. He has published more than 200 journal articles and 160 conference papers. His research interests include fuzzy neural networks, cerebellar model articulation controller, intelligent control systems, adaptive signal processing, and classification problem. He also serves as an Associate Editor for IEEE TRANSACTIONS ON CYBERNETICS and IEEE TRANSACTIONS ON FUZZY SYSTEMS.

DUC-HUNG PHAM was born in Hung Yen, Vietnam, in 1983. He received the B.S. degree in automatic control and the M.S. degree in automation from the Hanoi University of Science and Technology, Vietnam, in 2006 and 2011, respectively. He is currently pursuing the Ph.D. degree with the Department of Electrical Engineering, Yuan Ze University, Chung-Li, Taiwan. He is also a Lecturer with the Faculty of Electrical and Electronic, Hung Yen University of Technical and Education, Vietnam. His research interests include fuzzy logic control, neural networks, cerebellar model articulation controller, brain emotional learning-based intelligent controller, and secure communication.

TUAN-TU HUYNH (Member, IEEE) was born in Ho Chi Minh City, Vietnam, in 1982. He received the B.S. degree in electrical and electronics from the Department of Electrical and Electronics Engineering, Ho Chi Minh University of Technology and Education, Vietnam, in 2005, the M.S. degree in automation from the Ho Chi Minh City University of Transport, Vietnam, in 2010, and the Ph.D. degree in electrical engineering from Yuan Ze University, Taoyuan, Taiwan, in 2018. He is currently a Research Fellow with the Department of Electrical Engineering, Yuan Ze University, Chung-Li, Taiwan. He is also a Lecturer with the Faculty of Mechatronics and Electronics, Lac Hong University, Vietnam. His research interests include MCDM, fuzzy logic control, neural networks, cerebellar model articulation controller, brain emotional learning-based intelligent controller, deep learning, and intelligent control systems.