



Secure Communication Scheme for Brain-Computer Interface Systems Based on High-Dimensional Hyperbolic Sine Chaotic System

Xiangzi Zhang^{1,2}, Xiaobin Ding^{1,2}, Dandan Tong^{1,2}, Pengbin Chang³ and Jizhao Liu^{4*}

¹School of Psychology, Northwest Normal University, Lanzhou, China, ²Key Laboratory of and Mental Health of Gansu Province, Northwest Normal University, Lanzhou, China, ³Lanzhou University Science Park, Lanzhou University, Lanzhou, China, ⁴School of Information Science and Engineering, Lanzhou University, Lanzhou, China

Brain-Computer Interface (BCI) is a direct communication pathway between the brain and the external environment without using peripheral nerves and muscles. This emerging topic is suffering from serious issues such as malicious tampering and privacy leakage. To address this issue, we propose a novel communication scheme for BCI Systems. In particular, this scheme first utilizes high-dimensional chaotic systems with hyperbolic sine nonlinearity as the random number generator, then decorrelation operation is used to remove the physical characteristics of the output sequences. Finally, each of the sequences is applied in differential chaos shift keying (DCSK). Since each output sequence corresponds to a unique electrode, the communication data of different electrodes will not interfere with each other. Compared with popular multi-user DSK schemes using Walsh code sequences, this scheme does not require the channel data of all electrodes while decoding. Therefore, this scheme has higher efficiency. Experimental results on communication data indicate that the proposed scheme can provide a high level of security.

OPEN ACCESS

Edited by:

Qiang Lai,
East China Jiaotong University, China

Reviewed by:

Hegui Zhu,
Northeastern University, China
Qingchun Zhao,
Northeastern University, China

*Correspondence:

Jizhao Liu
liujz@lzu.edu.cn

Specialty section:

This article was submitted to
Interdisciplinary Physics,
a section of the journal
Frontiers in Physics

Received: 01 November 2021

Accepted: 07 December 2021

Published: 10 January 2022

Citation:

Zhang X, Ding X, Tong D, Chang P and
Liu J (2022) Secure Communication
Scheme for Brain-Computer Interface
Systems Based on High-Dimensional
Hyperbolic Sine Chaotic System.
Front. Phys. 9:806647.
doi: 10.3389/fphy.2021.806647

Keywords: secure communication scheme, BCI system, chaotic system, privacy protection, DCSK

INTRODUCTION

Brain-computer interface (BCI) is a real-time communication system in which messages or commands sent by the user do not pass through the brain's natural output pathways [1]. This technology provides a new way of brain monitoring, human-computer interaction, and it has broad applications in medical rehabilitation and other fields [2]. The representative works of BCI systems mainly involve two paths [3]. The first path is the realization of information exchange and control with the external environment by directly decoding the brain's instructions [4]. Such applications like BCI-based cursor system [5], robotic arm [6], wheelchair [7], text input method [8] help disabled patients to control external devices without using peripheral nerves and muscles. The second path is rehabilitation, enhancement, and improvement of the central nervous system [9]. By using BCI systems, new rehabilitation paradigms are proposed to help patients to recover from nervous system disease. Such BCI auxiliary training strategy can benefit stroke rehabilitation training [10] and spinal injury rehabilitation training [11].

Most of the above BCI systems use plain-text to transmit EEG data, which have serious issues such as malicious tampering and privacy leakage [12, 13]. For example, an attacker can easily decode the

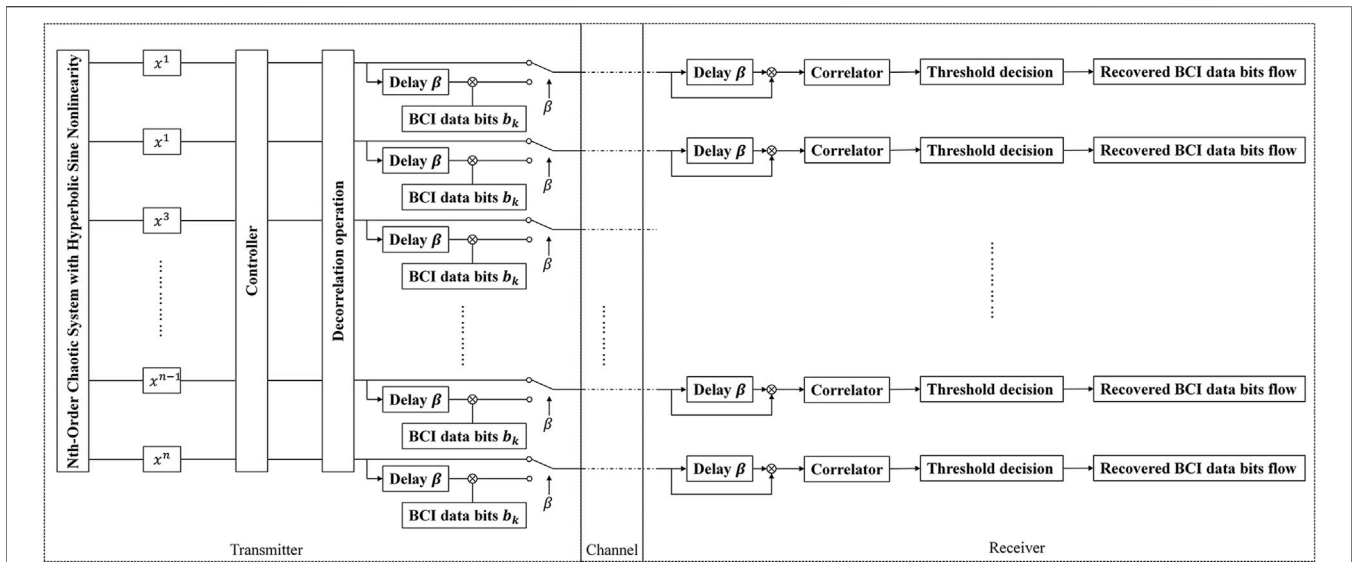


FIGURE 1 | Overall flowchart of High dimensional multi user DCSK scheme (HD-MU-DCSK).

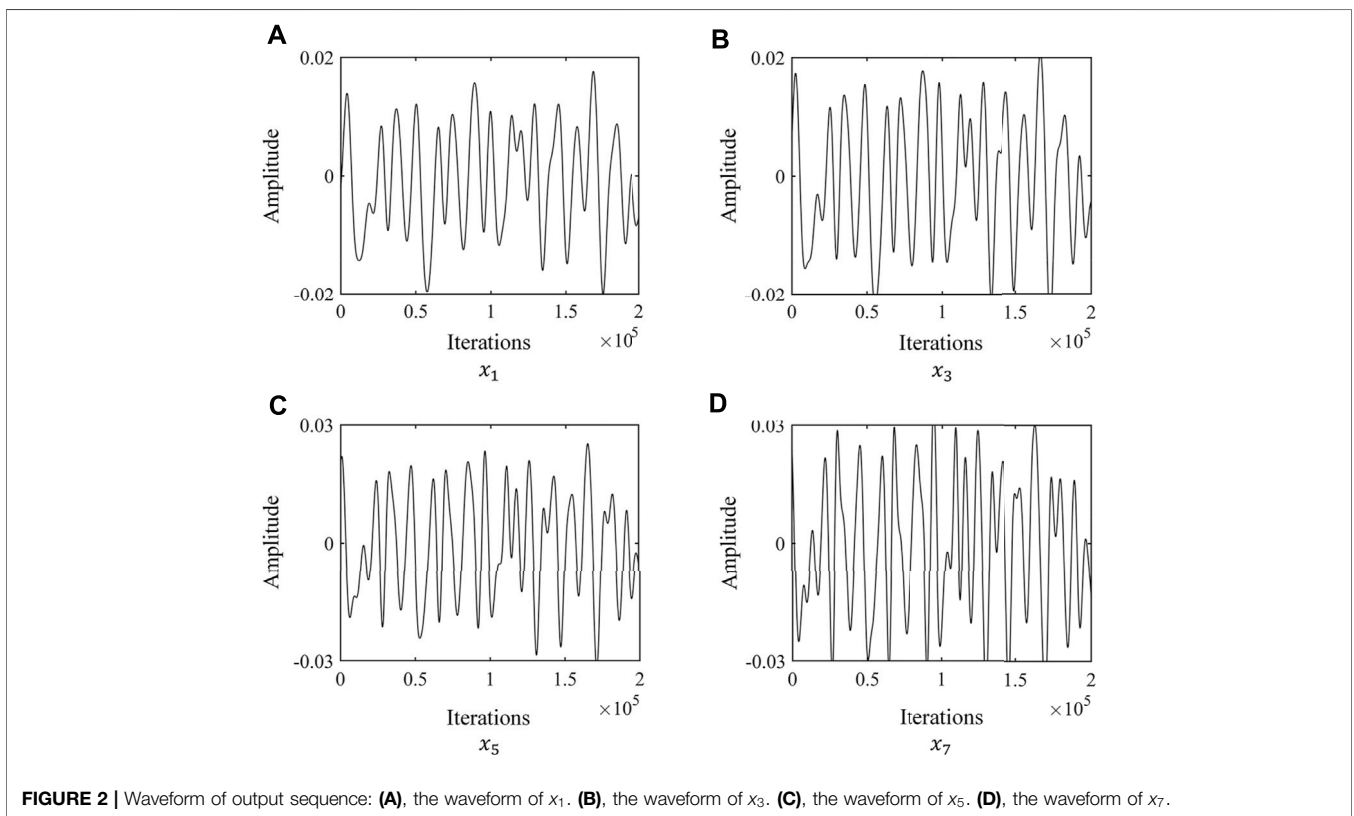
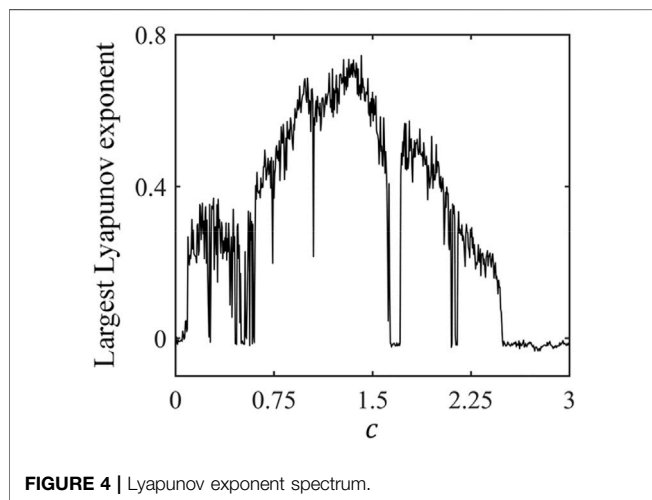
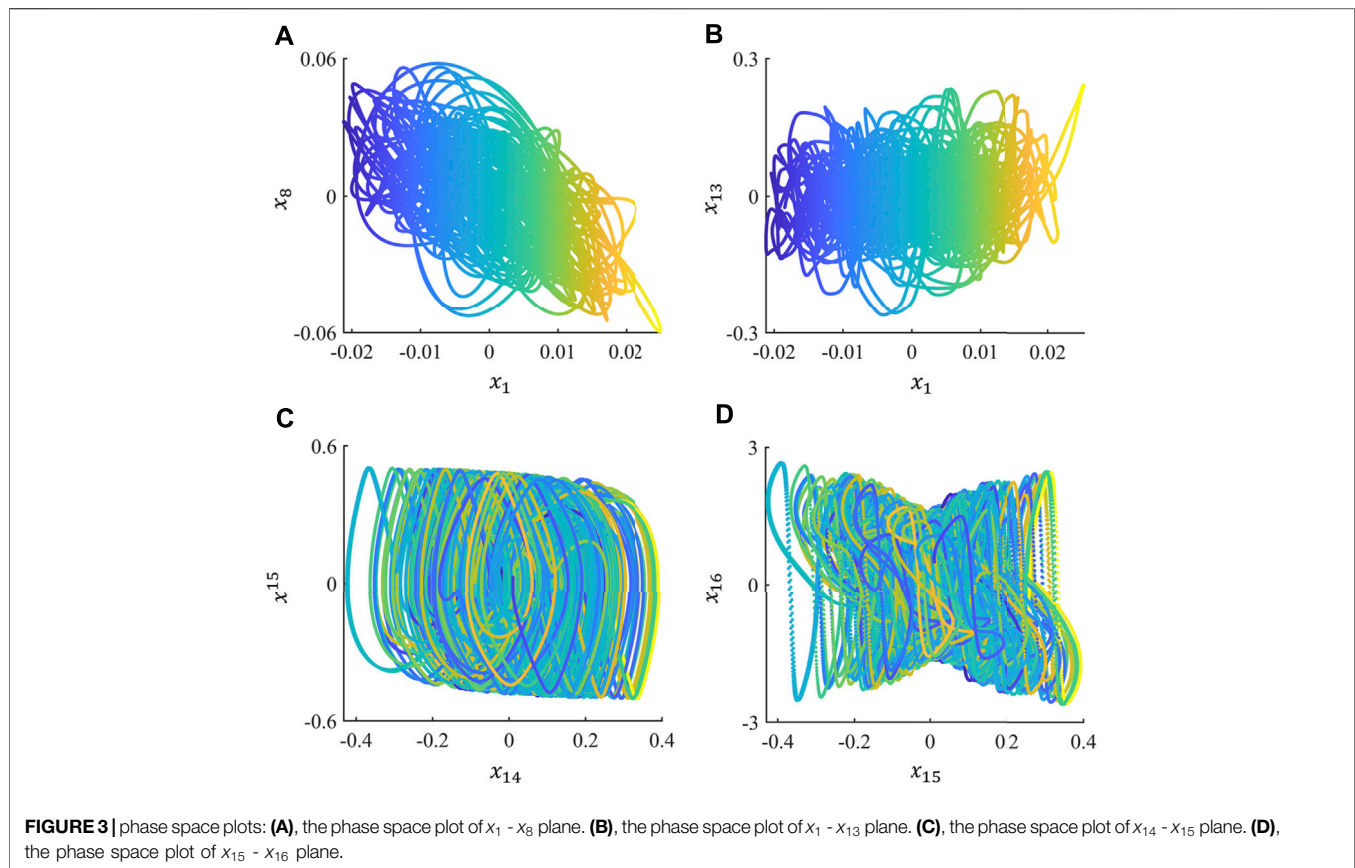


FIGURE 2 | Waveform of output sequence: (A), the waveform of x_1 . (B), the waveform of x_3 . (C), the waveform of x_5 . (D), the waveform of x_7 .

commands from the brain and control the device through tampering [14]. For BCI-based rehabilitation methods, malicious tampering can aggravate the patient’s condition [15]. Therefore, the communication data need to be encrypted to prevent the BCI systems from threats.

The basic communication system consists of an information source and an information sink connected by a channel. Unlike image data or video data, EEG is a high-dimensional and continuous data flow [16]. In BCI systems, the EEG data are collected by the electrode and then converted to digital signals by



the AD converter. Next, the digital EEG data flow are transmitted to the servers. The servers extract the features from the EEG signals and decode them to human commands. Considering those characteristics of EEG data and BCI systems, we designed a secure communication scheme to protect the transmissive EEG data flow. In particular, we applied a high-dimensional chaotic system of hyperbolic sine nonlinearity in the differential chaos shift keying (DCSK) scheme to prevent BCI systems from malicious tampering and privacy leakage [17].

DCSK is a chaos-based method for secure communication. Chaotic signals have many special characteristics, such as nonperiodicity, long-term unpredictability, wide spectrum, self- and cross-correlation characteristics [18, 19]. It is worth noting that the chaotic system will not only produce chaotic attractors, but also several independent attractors under certain parameters, that is, multiple coexisting attractors [20–22]. These characteristics meet the requirements of cryptosystem and secure communication system [23, 24]. A large number of literatures have proved that chaos-based image encryption schemes can provide high security and robustness, which can be used as a reliable image cryptosystem [25, 26].

Encryption is an effective way to protect data for information sources and an information sink, while secure communication scheme can protect the transmitted data in channel. DCSK is a secure communication scheme that employ non-periodic and wideband chaotic signals as carriers to achieve the effect of spectrum spreading in the process of digital modulation [27]. The reason why we use this route map is as follows: 1) The transmissive EEG data flow is a digital signal. There is no loss of EEG signal using the DCSK scheme for communication [28]. 2) The transmissive data in the DCSK scheme are the non-periodic chaotic signal or the modulated chaotic signal which can protect the EEG data from malicious tampering and privacy leakage [29]. 3) DCSK scheme is a simple method to achieve secure communication purposes without using chaos synchronization [30].

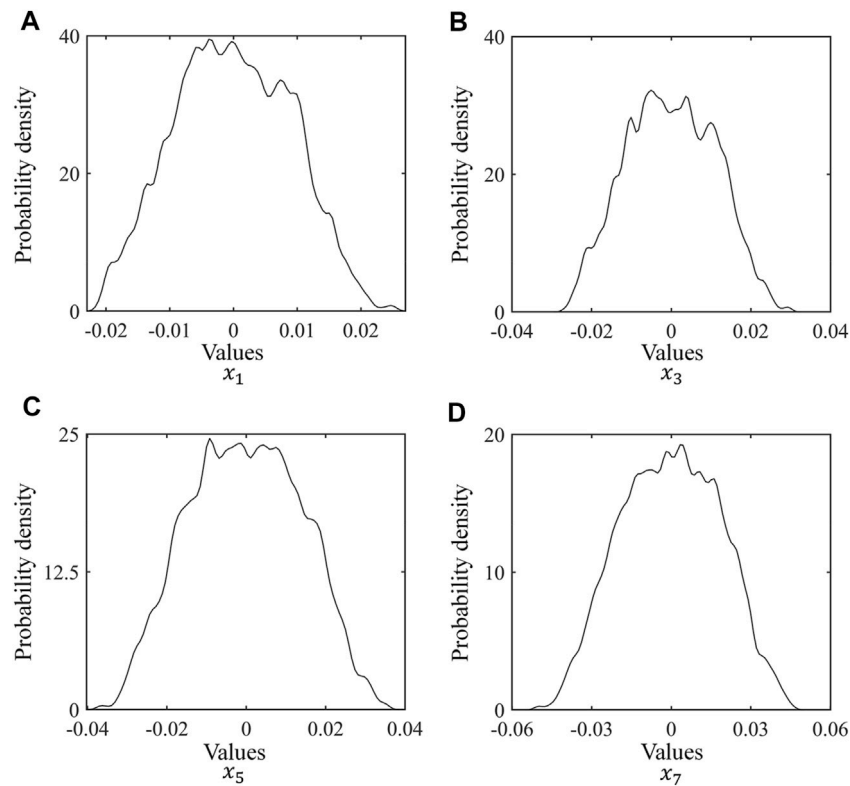


FIGURE 5 | Probability density distributions of output sequences. **(A)**, the probability density distributions of the output sequence x_1 . **(B)**, the probability density distributions of the output sequence x_3 . **(C)**, the probability density distributions of the output sequence x_5 . **(D)**, the probability density distributions of the output sequence x_7 .

Since the BCI system is a multi-channel system, the multi-user DCSK schemes are required to protect the EEG data flow. Kolumban et al. first combined the multi-user technology with the DCSK system [31]. In 2005, Frequency Modulated Efficient DCSK, FM-E-DCSK is proposed, which uses a reference signal to modulate multiple information signals to increase the transmission rate [32]. In 2016, Zhang et al. proposed Multi User Segment Shift Differential Chaos Shift Keying, MU-SSDCSK. According to the number of users, this scheme divides the reference signals into signal segments, and then shifts these signal segments and matches them with different Walsh codes to form mutually orthogonal carrying signals [33]. In recent years, the DCSK scheme using Walsh code has gradually become the mainstream multi-user DCSK scheme [34]. However, all the above multi-user DCSK schemes are not suitable for BCI system. This is because BCI system requires high calculation accuracy to extract features from EEG signals [35]. Multiplexing the transmission signal will reduce the accuracy of feature extraction [36]. Although using Walsh codes can solve this problem, it needs all the channels to decode the transmission signal, while BCI systems only use a few of the EEG signals to extract the features corresponding to the command. For example, Zhang et al. selected part of 64-channel for improving BCI illiteracy [37]. Atkinson et al. proposed an improving

BCI-based emotion recognition by using 14 channels of 32-electrode channels [38].

HIGH DIMENSIONAL MULTI USER DCSK SCHEME

To design an accurate and efficient secure communication scheme, we utilize high dimensional chaotic systems as the pseudo-random number generator, each variable corresponds to one channel which is used in the DCSK scheme. The flowchart is shown in **Figure 1**.

In this scheme, the controller selects the communication channel according to the corresponding BCI task. When a specific communication channel is selected, the channel first transmits a decorrelated chaotic sequence of length β as a reference signal, then transmits a multiplied modulated signal which has the same length as the decorrelated chaotic sequence. The modulation rule is described as follows:

$$S_i = \begin{cases} x_i & 2k\beta < i \leq (2k+1)\beta \\ b_k x_{i-\beta} & (2k+1)\beta < i \leq 2(k+1)\beta \end{cases} \quad (1)$$

Where x_i is the decorrelated chaotic sequence generated by a high dimensional chaotic system, b_k is the transmitted EEG data in

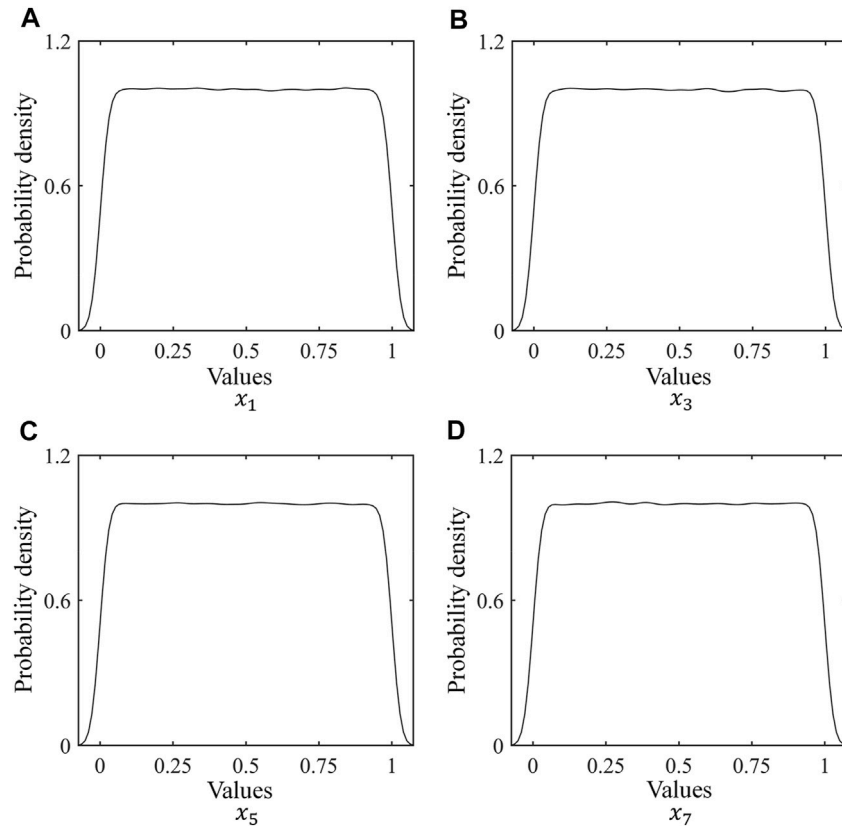


FIGURE 6 | Probability density distributions of output sequences after decorrelation operation. **(A)**, the probability density distributions of the above sequence x_1 . **(B)**, the probability density distributions of the above sequence x_3 . **(C)**, the probability density distributions of the above sequence x_5 . **(D)**, the probability density distributions of the above sequence x_7 .

BCI system, β is the time slot (length of the reference signal and modulated signal), k represents the iteration time.

For the demodulation process, the receiver calculates the correlation between the received signal r_i and the signal $r_{i-\beta}$, which is r_i delayed by β . The output of the correlator is:

$$Z_k = \sum_{(2k+1)\beta+1}^{2(k+1)\beta} r_i r_{i-\beta} \quad (2)$$

Therefore, the information bit b_k can be restored by the sign of the decision variable:

$$\hat{b}_k = \text{sgn}[Z_k] \quad (3)$$

The difficulty of this scheme is to design a high-dimensional chaotic system to generate the pseudo-random sequences. Reference [39] introduced a new and unified approach for designing desirable dissipative hyperchaotic systems. Reference [40] proposed a design method for generating hyperchaotic cat maps with any desired number of positive Lyapunov exponents. Our previous work proposed a simple method for generating n th order chaotic systems with hyperbolic sine nonlinearity [41]. The proposed scheme utilizes two back-to-back diodes representing hyperbolic sine nonlinearity without any multiplier or subcircuits. Therefore, the proposed high dimensional chaotic

systems can achieve both physical simplicity and analytic complexity at the same time.

SECURE COMMUNICATION SCHEME FOR BRAIN-COMPUTER INTERFACE BASED SPELLER AND MICROSLEEP DETECTOR

Here we applied the proposed scheme in BCI-based speller and microsleeper detector. Electroencephalography (EEG) -based P300 speller is a type of brain-computer interface (BCI) that uses EEG to allow a user to select characters without physical movement [42]. The EEG-based microsleeper detector uses BCI technology to detect drowsiness, which can benefit the drivers to avoid car accidents [43]. If the communication data of these BCI systems have been maliciously tampered, the attackers may cause some serious accidents.

The above BCI systems use 16-electrode to collect EEG signals. Therefore, it is needed to design a chaotic system that has sixteen dimensions. In this paper, EEG data were acquired from 16 scalp sites (extended 10–20 system) using a cap with active Ag/AgCl electrodes. Wet electrodes were used in the cap, and the electrode impedance was modulated to be less than 5 K Ω . The reference electrode was on the bilateral mastoid. A Neuroscan Synamps2

TABLE 1 | Pearson product-moment correlation coefficient of the two output sequences before decorrelation operation.

x16	x15	x14	x13	x12	x11	x10	x9	x8	x7	x6	x5	x4	x3	x2	x1	
0.0017	-0.0066	0.0564	0.1063	0.1209	0.0483	-0.1257	-0.3534	-0.5389	-0.5843	-0.44	-0.1283	0.2693	0.6463	0.9084	1	x1
0.0012	-0.0121	0.0631	0.1086	0.0823	-0.0578	-0.2841	-0.5009	-0.5921	-0.4838	-0.1838	0.2247	0.6224	0.902	1	0.9084	x2
-0.0018	-0.0154	0.0788	0.1023	0.0095	-0.2025	-0.4458	-0.5871	-0.5241	-0.2433	0.1739	0.5947	0.8946	1	0.902	0.6463	x3
-0.0076	-0.0079	0.0983	0.0682	-0.1122	-0.3733	-0.5672	-0.5587	-0.3062	0.1161	0.562	0.8858	1	0.8946	0.6224	0.2693	x4
-0.0144	0.0188	0.1015	-0.02	-0.2834	-0.5297	-0.5851	-0.3711	0.0516	0.5239	0.8752	1	0.8858	0.5947	0.2247	-0.1283	x5
-0.0182	0.0658	0.0559	-0.1781	-0.4711	-0.5998	-0.4361	-0.0191	0.4801	0.8627	1	0.8752	0.562	0.1739	-0.1838	-0.44	x6
-0.0132	0.1181	-0.0663	-0.3847	-0.5966	-0.4988	-0.0958	0.4308	0.8483	1	0.8627	0.5239	0.1161	-0.2433	-0.4838	-0.5843	x7
0.004	0.144	-0.2591	-0.5614	-0.5538	-0.1785	0.3748	0.8317	1	0.8483	0.4801	0.0516	-0.3062	-0.5241	-0.5921	-0.5389	x8
0.0315	0.106	-0.4581	-0.5856	-0.2658	0.3106	0.8123	1	0.8317	0.4308	-0.0191	-0.3711	-0.5587	-0.5871	-0.5009	-0.3534	x9
0.0626	-0.0163	-0.5467	-0.3507	0.2352	0.7889	1	0.8123	0.3748	-0.0958	-0.4361	-0.5851	-0.5672	-0.4458	-0.2841	-0.1257	x10
0.0868	-0.2097	-0.4056	0.1424	0.7588	1	0.7889	0.3106	-0.1785	-0.4988	-0.5998	-0.5297	-0.3733	-0.2025	-0.0578	0.0483	x11
0.067	-0.4218	0.0144	0.7129	1	0.7588	0.2352	-0.2658	-0.5538	-0.5966	-0.4711	-0.2834	-0.1122	0.0095	0.0823	0.1209	x12
-0.1225	-0.4909	0.6195	1	0.7129	0.1424	-0.3507	-0.5856	-0.5614	-0.3847	-0.1781	-0.02	0.0682	0.1023	0.1086	0.1063	x13
-0.5065	0.00003	1	0.6195	0.0144	-0.4056	-0.5467	-0.4581	-0.2591	-0.0663	0.0559	0.1015	0.0983	0.0788	0.0631	0.0564	x14
-0.0001	1	0.00003	-0.4909	-0.4218	-0.2097	-0.0163	0.106	0.144	0.1181	0.0658	0.0188	-0.0079	-0.0154	-0.0121	-0.0066	x15
1	-0.0001	-0.5065	-0.1225	0.067	0.0868	0.0626	0.0315	0.004	-0.0132	-0.0182	-0.0144	-0.0076	-0.0018	0.0012	0.0017	x16

TABLE 2 | Pearson product-moment correlation coefficient of the two output sequences after decorrelation operation.

x16	x15	x14	x13	x12	x11	x10	x9	x8	x7	x6	x5	x4	x3	x2	x1	
-0.0006	0.0009	0.00001	-0.00001	0.0002	-0.0006	-0.002	-0.0009	-0.0004	-0.0004	-0.0005	0.0004	-0.0007	0.0004	-0.0017	1	x1
-0.0007	-0.0015	0.0002	-0.0001	0.0031	0.0012	-0.0009	-0.0013	0.0018	0.0021	0.0014	0.0005	0.0006	-0.0004	1	-0.0017	x2
-0.0018	-0.0005	0.0009	0.0004	-0.0003	-0.0001	0.0022	0.0001	0.0007	-0.0016	-0.0003	0.0001	-0.0008	1	-0.0004	0.0004	x3
-0.0013	-0.0005	0.0004	0.0013	-0.0001	-0.0009	0.0005	-0.0004	-0.0001	0.0011	0.0015	-0.0011	1	-0.0008	0.0006	-0.0007	x4
0.0012	0.0005	-0.0011	0.0004	-0.0006	0.0003	-0.0001	0.0008	-0.0002	-0.0002	0.001	1	-0.0011	0.0001	0.0005	0.0004	x5
0.001	-0.0005	0.0007	-0.0009	-0.0002	-0.0007	0.0004	-0.0003	0.0005	0.0005	1	0.001	0.0015	-0.0003	0.0014	-0.0005	x6
-0.0011	0.0008	0.0007	-0.0007	0.0015	0.0024	0.00003	-0.0015	-0.0009	1	0.0005	-0.0002	0.0011	-0.0016	0.0021	-0.0004	x7
-0.0029	0.0017	0.001	-0.0004	-0.0008	-0.0001	0.001	-0.0002	1	-0.0009	0.0005	-0.0002	-0.0001	0.0007	0.0018	-0.0004	x8
0.0002	0.0009	0.0002	0.0019	-0.0001	0.0005	0.0001	1	-0.0002	-0.0015	-0.0003	0.0008	-0.0004	0.0001	-0.0013	-0.0009	x9
-0.0006	0.0009	-0.0002	0.0004	-0.0001	-0.0011	1	0.0001	0.001	0.00003	0.0004	-0.0001	0.0005	0.0022	-0.0009	-0.002	x10
0.0014	0.0019	-0.0007	-0.0012	0.0001	1	-0.0011	0.0005	-0.0001	0.0024	-0.0007	0.0003	-0.0009	-0.0001	0.0012	-0.0006	x11
0.0017	-0.0003	0.001	-0.0028	1	0.0001	-0.0001	-0.0001	-0.0008	0.0015	-0.0002	-0.0006	-0.0001	-0.0003	0.0031	0.0002	x12
0.0017	0.0002	0.0007	1	-0.0028	-0.0012	0.0004	0.0019	-0.0004	-0.0007	-0.0009	0.0004	0.0013	0.0004	-0.0001	-0.00001	x13
0.0004	0.0017	1	0.0007	0.001	-0.0007	-0.0002	0.0002	0.001	0.0007	0.0007	-0.0011	0.0004	0.0009	0.0002	0.00001	x14
0.0014	1	0.0017	0.0002	-0.0003	0.0019	0.0009	0.0009	0.0017	0.0008	-0.0005	0.0005	-0.0005	-0.0005	-0.0015	0.0009	x15
1	0.0014	0.0004	0.0017	0.0017	0.0014	-0.0006	0.0002	-0.0029	-0.0011	0.001	0.0012	-0.0013	-0.0018	-0.0007	-0.0006	x16

TABLE 3 | Results of SP 800–22 test using x_1 after decorrelation operation.

Test	p-value	Result
Approximate Entropy	0.098853	Success
Block Frequency	0.94943	Success
Cumulative Sums	0.392,502	Success
FFT	0.978,037	Success
Frequency	0.252,624	Success
Linear Complexity	0.906,511	Success
Longest Run	0.443,146	Success
Non-Overlapping Template	0.361,567	Success
Overlapping Template	1	Success
Random Excursions	0.05684	Success
Random Excursions Variant	0.627,287	Success
Rank	0.659,889	Success
Runs	0.668,711	Success
Serial	0.093027	Success
Universal	0.141,508	Success

TABLE 6 | Results of SP 800–22 test using x_7 after decorrelation operation.

Test	p-value	Result
Approximate Entropy	0.846,242	Success
Block Frequency	0.904,758	Success
Cumulative Sums	0.689,519	Success
FFT	0.832,839	Success
Frequency	0.523,474	Success
Linear Complexity	0.651,641	Success
Longest Run	0.276,194	Success
Non-Overlapping Template	0.07046	Success
Overlapping Template	0.051553	Success
Random Excursions	0.150,568	Success
Random Excursions Variant	0.616,838	Success
Rank	0.644,792	Success
Runs	0.900,739	Success
Serial	0.834,662	Success
Universal	0.881,265	Success

TABLE 4 | Results of SP 800–22 test using x_3 after decorrelation operation.

Test	p-value	Result
Approximate Entropy	1	Success
Block Frequency	0.930,814	Success
Cumulative Sums	0.545,722	Success
FFT	0.201,659	Success
Frequency	0.352,521	Success
Linear Complexity	0.516,151	Success
Longest Run	0.113,107	Success
Non-Overlapping Template	0.257,712	Success
Overlapping Template	1	Success
Random Excursions	0.394,639	Success
Random Excursions Variant	0.785,267	Success
Rank	0.82942	Success
Runs	0.180,869	Success
Serial	0.485,295	Success
Universal	0.822,527	Success

TABLE 5 | Results of SP 800–22 test using x_5 after decorrelation operation.

Test	p-value	Result
Approximate Entropy	0.831,444	Success
Block Frequency	0.774,929	Success
Cumulative Sums	0.390,633	Success
FFT	0.516,412	Success
Frequency	0.439,182	Success
Linear Complexity	0.784,995	Success
Longest Run	0.159,788	Success
Non-Overlapping Template	0.186,118	Success
Overlapping Template	0.054513	Success
Random Excursions	0.301,755	Success
Random Excursions Variant	0.723,645	Success
Rank	0.142,671	Success
Runs	0.585,076	Success
Serial	0.978,004	Success
Universal	0.854,829	Success

amplifier amplified the EEG signal. The sampling rate of the EEG signal was 1 kHz. We collected EEG data of subjects performing ballistic index finger abduction movements [28], and the data length is about 15 min.

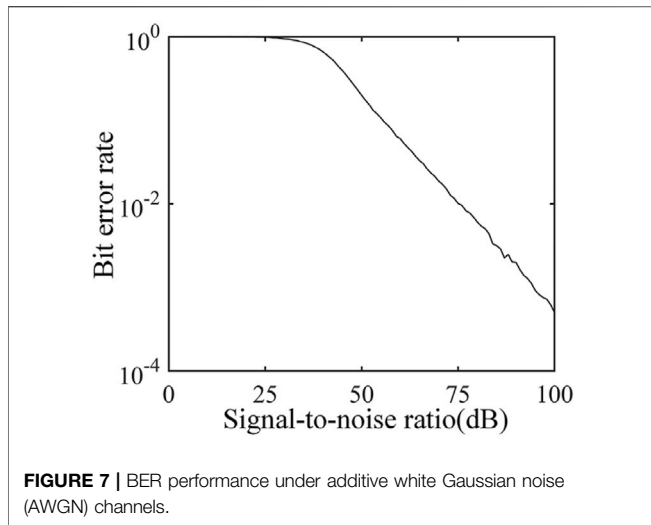
16th-Order Hyperbolic Sine Chaotic System

Based on the design method proposed in Ref. [41], we proposed the 16th-order hyperbolic sine chaotic system, which is described as follows:

$$\begin{cases}
 \dot{x}_1 = x_2 - x_1 \\
 \dot{x}_2 = x_3 - x_2 \\
 \dot{x}_3 = x_4 - x_3 \\
 \dot{x}_4 = x_5 - x_4 \\
 \dot{x}_5 = x_6 - x_5 \\
 \dot{x}_6 = x_7 - x_6 \\
 \dot{x}_7 = x_8 - x_7 \\
 \dot{x}_8 = x_9 - x_8 \\
 \dot{x}_9 = x_{10} - x_9 \\
 \dot{x}_{10} = x_{11} - x_{10} \\
 \dot{x}_{11} = x_{12} - x_{11} \\
 \dot{x}_{12} = x_{13} - x_{12} \\
 \dot{x}_{13} = x_{14} - x_{13} \\
 \dot{x}_{14} = x_{15} \\
 \dot{x}_{15} = x_{16} \\
 \dot{x}_{16} = cx_{16} - \rho \sinh(\varphi x_{15}) - 16x_{14} - 16x_{13} - 16x_{12} - 16x_{11} \\
 \quad - 16x_{10} - 16x_9 - 16x_8 - 16x_7 - 16x_6 - 16x_5 - 16x_4 - 16x_3 \\
 \quad - 16x_2 - \frac{1}{32}x_1
 \end{cases} \tag{4}$$

When $c = 1$, the system exhibits chaotic behavior, the waveform is shown as **Figure 2**, the phase space plot is shown in **Figure 3**.

To study the overall dynamic behavior of the proposed system, we plot the Largest Lyapunov exponent spectrum. Lyapunov exponent is a measure of a system’s predictability and sensitivity to changes in its initial conditions. If the largest Lyapunov exponent (LLE) is greater than zero, the system exhibits chaotic behavior. If $LLE = 0$, the system exhibits periodic behavior. If $LLE < 0$, the system converges to a stable



point. When $c = [0, 3]$, The largest Lyapunov exponent spectrum is shown as **Figure 4**.

From **Figure 4**, the chaos exists in $c \in [0.07 - 2.49]$ except some period windows are embedded.

PHYSICAL CHARACTERISTICS OF THE OUTPUT SEQUENCE

Although the proposed system can generate pseudo-random sequences, it has physical characteristics [45], **Figure 5** is the probability density distributions of the output sequence x_1, x_3, x_5, x_7 .

From the results of **Figure 5**, the output sequences have physical characteristics. Therefore, it may be cracked by the side-channel attack. To remove the physical characteristics, we utilize the decorrelation operation:

$$S_{out} = S_{in} * 10^5 - \text{floor}(S_{in} * 10^5) \quad (5)$$

The probability density distributions of the above sequences after decorrelation operation are plotted in **Figure 6**.

EXPERIMENTS

This section is the performance analysis of the proposed scheme, which includes mutual interference suppression, security, bit error rate, and time efficiency.

MUTUAL INTERFERENCE BETWEEN CHANNELS

The decorrelation operation not only can remove the physical characteristics, but also can suppress mutual interference between channels. We test the Pearson product-moment correlation

TABLE 7 | Results of time and speed of the scheme.

Index	Time, s	Speed, kb/s
Generation of Carrier signal	29.864	33.485
Modulation	0.250	4,000
Demodulation	0.278	3,597.122

coefficient (PPMCC) of 10^5 data of two output sequences. The comparative results are shown in **Tables 1, 2**.

From the results in **Table 1**. Most PPMCCs are greater than 0.4, some PPMCC like $x_1 \sim x_2, x_2 \sim x_3$ are over 0.9, which means the original sequences have strong correlation. From the results in **Table 2**, PPMCC after decorrelation are less than 0.01, which means the sequences after decorrelation operation have strong interference suppression ability, the communication data flow of different channels will not interfere with each other, which ensures that the BCI systems can accurately extract EEG features.

KEY SPACE ANALYSIS

If the attackers have all the details of the HD-MU-DCSK scheme, this communication protocol will no longer be secure. In this circumstance, the defender can improve the security by frequently changing the secure key. For **Eq. 4**, all initial conditions and control parameters can set to be the secure keys. As shown in **Figure 4**, chaos exists in $c \in [0.05, 2.49]$. Suppose all initial conditions and control parameters are equal, the key space will be larger than $(5.68 \times 10^9)^{59} \gg 10^{531}$ (for 32-bit system), if the defender changes secure key every second, the keys can be used for over 3.17×10^{58} years. Therefore, the proposed scheme can provide high security level.

SECURITY ANALYSIS

Security is the most important performance considered in this work. To evaluate the data security of the proposed scheme, we use the standard statistical test suite (SP 800-22) for random number generators provided by the National Institute of Standard Technology (NIST). The test results of the output sequence x_1 after decorrelation operation is shown in **Table 3**.

From **Tables 3–6**, the output sequence x_1, x_3, x_5 , and x_7 after decorrelation operation can pass all of the NIST tests. Therefore, it can provide a high level of security when these sequences as the carrier signal.

BIT ERROR RATE

The proposed scheme can carry out secure communication under noisy channels. The performance of the bit error rate is shown in **Figure 7**.

TIME EFFICIENCY

We have tested 10^6 bit data to evaluate the time efficiency performance of the proposed scheme. The computer configuration used in this test is i5-8,265 processor (8-core, 1.60 GHz) with 8 GB memory. The average detailed results are shown in **Table 7**.

From the testing results of time efficiency performance, the main factor restricting the speed of this scheme is the generation of chaotic sequences. This is because we utilize Fourth-order Runge-Kutta algorithm to generate the output sequence, each iteration time requires 80 iterations. If a circuit or FPGA is used to generate high-speed pseudo-random numbers, this problem can be solved.

CONCLUSION AND FUTURE WORK

In this work, we proposed a secure communication scheme for BCI systems based on high-dimensional hyperbolic sine chaotic systems. The testing results indicate that the proposed scheme can provide a high level of security. The communication data between the electrodes will not cause mutual interference. For the time efficiency of the proposed scheme, the generation of the pseudo-random sequences is the bottleneck restricting the execution speed of the scheme. Designing the corresponding circuit or FPGA system can solve this bottleneck.

REFERENCES

1. Wolpaw JR, Birbaumer N, Heetderks WJ, McFarland DJ, Peckham PH, Schalk G, et al. Brain-computer Interface Technology: a Review of the First International Meeting. *IEEE Trans Rehab Eng* (2000) 8(2):164–73. doi:10.1109/tre.2000.847807
2. Ortiz M, Iáñez E, Gaxiola-Tirado JA, Gutiérrez D, Azorín JM. Study of the Functional Brain Connectivity and Lower-Limb Motor Imagery Performance after Transcranial Direct Current Stimulation. *Int J Neur Syst* (2020) 30(08):2050038. doi:10.1142/s0129065720500380
3. Mühl C, Allison B, Nijholt A, Chanel G. A Survey of Affective Brain Computer Interfaces: Principles, State-Of-The-Art, and Challenges[J]. *Brain-Computer Inter* (2014) 1(2):66–84.
4. Wolpaw JR, McFarland DJ, Vaughan TM, Schalk G. The Wadsworth Center Brain-Computer Interface (BCI) Research and Development Program. *IEEE Trans Neural Syst Rehabil Eng* (2003) 11(2):1–4. doi:10.1109/tnsre.2003.814442
5. Rohani DA, Sorensen HBD, Puthusserypady S. In: Brain-computer interface using P300 and virtual reality: A gaming approach for treating ADHD[C]//2014 36th Annual International Conference of the IEEE Engineering in Medicine and Biology Society. IEEE (2014). p. 3606–9.
6. Hsu W-Y. Continuous Eeg Signal Analysis for Asynchronous Bci Application. *Int J Neur Syst* (2011) 21(04):335–50. doi:10.1142/s0129065711002870
7. Wolpaw JR, Birbaumer N, McFarland DJ, Pfurtscheller G, Vaughan TM. Brain-computer Interfaces for Communication and Control. *Clin Neurophysiol* (2002) 113(6):767–91. doi:10.1016/s1388-2457(02)00057-3
8. Dobkin BH. Brain-computer Interface Technology as a Tool to Augment Plasticity and Outcomes for Neurological Rehabilitation. *J Physiol* (2007) 579(3):637–42. doi:10.1113/jphysiol.2006.123067
9. Daly JJ, Huggins JE. Brain-Computer Interface: Current and Emerging Rehabilitation Applications. *Arch Phys Med Rehabil* (2015) 96(3):S1–S7. doi:10.1016/j.apmr.2015.01.007
10. Yang S, Li R, Li H, Xu K, Shi Y, Wang Q, et al. Exploring the Use of Brain-Computer Interfaces in Stroke Neurorehabilitation. *Biomed Res Int* (2021) 2021:9967348. doi:10.1155/2021/9967348

DATA AVAILABILITY STATEMENT

The original contributions presented in the study are included in the article/Supplementary Material, further inquiries can be directed to the corresponding author.

AUTHOR CONTRIBUTIONS

XZ raises the issue of security risks of BCI systems. JL designed the secure communication scheme. XZ, XD, DT, and PC performed the experiments. JL wrote the paper. All authors have proposed amendments to the manuscript.

FUNDING

This study is supported by the Natural Science Foundation of Gansu Province (No. 21JR7RA510), and Distinguished Young Scholars of Gansu Province of China (No. 21JR7RA345).

ACKNOWLEDGMENTS

The authors would like to thank Jing Lian for the helpful suggestions.

11. Broetz D, Braun C, Weber C, Soekadar SR, Caria A, Birbaumer N. Combination of Brain-Computer Interface Training and Goal-Directed Physical Therapy in Chronic Stroke: A Case Report. *Neurorehabil Neural Repair* (2010) 24(7):674–9. doi:10.1177/1545968310368683
12. Landau O, Cohen A, Gordon S, Nissim N. Mind Your Privacy: Privacy Leakage through BCI Applications Using Machine Learning Methods. *Knowledge-Based Syst* (2020) 198:105932. doi:10.1016/j.knsys.2020.105932
13. Zhu H, Guo Y, Zhang L. An Improved Convolution Merkle Tree-Based Blockchain Electronic Medical Record Secure Storage Scheme. *J Inf Security Appl* (2021) 61:102952. doi:10.1016/j.jisa.2021.102952
14. Takabi H, Bhalotiya A, Alohaly M. In: Brain computer interface (BCI) applications: Privacy threats and countermeasures[C]//2016 IEEE 2nd International Conference on Collaboration and Internet Computing (CIC). IEEE (2016). p. 102–11.
15. Li QQ, Ding D, Conti M. In: Brain-computer interface applications: Security and privacy challenges[C]//2015 IEEE Conference on Communications and Network Security (CNS). IEEE (2015). p. 663–6.
16. Yang F, Zhao X, Jiang W, Gao P, Liu G. Multi-method Fusion of Cross-Subject Emotion Recognition Based on High-Dimensional EEG Features. *Front Comput Neurosci* (2019) 13:53. doi:10.3389/fncom.2019.00053
17. Liu J, Clinton Sprott J, Wang S, Ma Y. Simplest Chaotic System with a Hyperbolic Sine and its Applications in DCSK Scheme. *IET Commun* (2018) 12(7):809–15. doi:10.1049/iet-com.2017.0455
18. Xiong L, Zhang X, Teng S, Qi L, Zhang P. Detecting Weak Signals by Using Memristor-Involved Chua's Circuit and Verification in Experimental Platform. *Int J Bifurcation Chaos* (2020) 30(13):2050193. doi:10.1142/s021812742050193x
19. Ma C, Mou J, Xiong L, Banerjee S, Liu T, Han X. Dynamical Analysis of a New Chaotic System: Asymmetric Multistability, Offset Boosting Control and Circuit Realization. *Nonlinear Dyn* (2021) 103(3):2867–80. doi:10.1007/s11071-021-06276-8
20. Lai Q. A Unified Chaotic System with Various Coexisting Attractors. *Int J Bifurcation Chaos* (2021) 31(01):2150013. doi:10.1142/s0218127421500139
21. Lai Q, Wan Z, Kengne LK, Kamdem Kuate PD, Chen C. Two-memristor-based Chaotic System with Infinite Coexisting Attractors[J]. *IEEE Trans Circuits Syst Express Briefs* (2020) 68(6):2197–201. doi:10.1109/tcsii.2020.3044096

22. Lai Q, Wan Z, Kamdem Kuate PD. Modelling and Circuit Realisation of a New No-Equilibrium Chaotic System with Hidden Attractor and Coexisting Attractors. *Electron Lett* (2020) 56(20):1044–6. doi:10.1049/el.2020.1630
23. Zhu H, Dai L, Liu Y, Wu L. A Three-Dimensional Bit-Level Image Encryption Algorithm with Rubik's Cube Method. *Mathematics Comput Simulation* (2021) 185:754–70. doi:10.1016/j.matcom.2021.02.009
24. Li X, Mou J, Xiong L, Wang Z, Xu J. Fractional-order Double-Ring Erbium-Doped Fiber Laser Chaotic System and its Application on Image Encryption. *Opt Laser Tech* (2021) 140:107074. doi:10.1016/j.optlastec.2021.107074
25. Zhu H, Zhao Y, Song Y. 2D Logistic-Modulated-Sine-Coupling-Logistic Chaotic Map for Image Encryption. *IEEE Access* (2019) 7:14081–98. doi:10.1109/access.2019.2893538
26. Zhu H, Zhang X, Yu H, Zhao C, Zhu Z. An Image Encryption Algorithm Based on Compound Homogeneous Hyper-Chaotic System. *Nonlinear Dyn* (2017) 89(1):61–79. doi:10.1007/s11071-017-3436-y
27. Luo R, Yang H, Meng C, Zhang X. A Novel SR-DCSK-Based Ambient Backscatter Communication System[J]. *IEEE Trans Circuits Syst Express Briefs* (2021) 1. doi:10.1109/tcsii.2021.3109020
28. Zhang X, Li H, Xie T, Liu Y, Chen J, Long J. Movement Speed Effects on Beta-Band Oscillations in Sensorimotor Cortex during Voluntary Activity. *J Neurophysiol* (2020) 124(2):352–9. doi:10.1152/jn.00238.2020
29. Cai X, Xu W, Hong S, Wang L. Discrete W Transform Based Index-Keying M-Ary DCSK for Non-coherent Chaotic Communications. *IEEE Commun Lett* (2021) 25(9):3104–8. doi:10.1109/lcomm.2021.3095075
30. Caplignis F, Litvinenko A, Aboltins A, Austrum E, Rusins A Chaotic Jerk Circuit Usage in Communication Systems[C]//2020 IEEE Microwave Theory and Techniques in Wireless Communications (MTTW). *IEEE* (2020) 1:227–30.
31. Kolubnan G, Kennedy MP, Jako Z, Kis G. Chaotic Communications with Correlator Receivers: Theory and Performance Limits. *Proc IEEE* (2002) 90(5): 711–32. doi:10.1109/jproc.2002.1015003
32. Qiu HB, Wang M. Analysis of the System Character of FM-EDCSK[J]. *Journal-China Inst Commun* (2005) 26(5):113. doi:10.3321/j.issn:1000-436X.2005.05.018
33. Zhang G, Zhao C, Zhang T. Performance Analysis of MISO-MU-OHE-DCSK System over Rayleigh Fading Channels. *AEU - Int J Elect Commun* (2020) 115: 153048. doi:10.1016/j.aeue.2019.153048
34. Chen P, Wang L, Chen G. DDCSK-walsh Coding: A Reliable Chaotic Modulation-Based Transmission Technique. *IEEE Trans Circuits Syst* (2012) 59(2):128–32. doi:10.1109/tcsii.2011.2180109
35. Zhang X, Guo Y, Gao B, Long J. In: Enhancing Mu-based BCI performance with rhythmic electrical stimulation at alpha frequency[C]//2019 41st Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC). *IEEE* (2019). p. 5540–3. doi:10.1109/EMBC.2019.8857321
36. Li S, Zhao Y, He L, Wu Z, Li Y. In: Design and performance analysis of a GFDM-DCSK communication system[C]//2016 13th IEEE Annual Consumer Communications & Networking Conference (CCNC). *IEEE* (2016). p. 802–3.
37. Zhang X, Guo Y, Gao B, Long J. Alpha Frequency Intervention by Electrical Stimulation to Improve Performance in Mu-Based BCI. *IEEE Trans Neural Syst Rehabil Eng* (2020) 28(6):1262–70. doi:10.1109/tnsre.2020.2987529
38. Atkinson J, Campos D. Improving BCI-Based Emotion Recognition by Combining EEG Feature Selection and Kernel Classifiers. *Expert Syst Appl* (2016) 47:35–41. doi:10.1016/j.eswa.2015.10.049
39. Shen C, Yu S, Lu J, Chen G. Designing Hyperchaotic Systems with Any Desired Number of Positive Lyapunov Exponents via A Simple Model. *IEEE Trans Circuits Syst* (2014) 61(8):2380–9. doi:10.1109/tcsi.2014.2304655
40. Wu Y, Hua Z, Zhou Y. \mathbb{S}^n -Dimensional Discrete Cat Map Generation Using Laplace Expansions. *IEEE Trans Cybern* (2015) 46(11):2622–33. doi:10.1109/TCYB.2015.2483621
41. Liu J, Ma J, Lian J, Chang P, Ma Y. An Approach for the Generation of an Nth-Order Chaotic System with Hyperbolic Sine. *Entropy* (2018) 20(4):230. doi:10.3390/e20040230
42. McCann MT, Thompson DE, Syed ZH, Huggins JE. Electrode Subset Selection Methods for an EEG-Based P300 Brain-Computer Interface. *Disabil Rehabil Assistive Tech* (2015) 10(3):216–20. doi:10.3109/17483107.2014.884174
43. Putra AE, Atmaji C, Utami TG. In: EEG-based microsleep detector using microcontroller[C]//2016 8th International Conference on Information Technology and Electrical Engineering (ICITEE). *IEEE* (2016). p. 1–4.
44. Liu J, Zhang X, Zhao Q, Lian J, Huang F, Ma Y. A Torus-Chaotic System and its Pseudorandom Properties[J]. *Complexity* (2020) 2020:1–12. doi:10.1155/2020/8315658

Conflict of Interest: The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Publisher's Note: All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers. Any product that may be evaluated in this article, or claim that may be made by its manufacturer, is not guaranteed or endorsed by the publisher.

Copyright © 2022 Zhang, Ding, Tong, Chang and Liu. This is an open-access article distributed under the terms of the Creative Commons Attribution License (CC BY). The use, distribution or reproduction in other forums is permitted, provided the original author(s) and the copyright owner(s) are credited and that the original publication in this journal is cited, in accordance with accepted academic practice. No use, distribution or reproduction is permitted which does not comply with these terms.