TYPE Original Research
PUBLISHED 18 May 2023
DOI 10.3389/fnins.2023.1174096

A data security scheme based on EEG characteristics for body area networks

Tong Bai[1†], Yuhao Jiang[1†], Jiazhang Yang[2], Jiasai Luo[1]* and Ya Du[3]*

[1] School of Optoelectronic Engineering, Chongqing University of Posts and Telecommunications, Chongqing, China, [2] The Women and Children Hospital of Yongchuan, Chongqing, China, [3] Department of Peripheral Vascular (Wound Repair), Chongqing Hospital of Traditional Chinese Medicine, Chongqing, China

OPEN ACCESS

EDITED BY
Xiaomin Yang,
Sichuan University, China

REVIEWED BY
Tianhan Li,
Xinxiang Medical University, China
Wuzhong Yin,
Southwest University of Science and Technology, China

*CORRESPONDENCE
Jiasai Luo
✉ luojs@cqupt.edu.cn
Ya Du
✉ 361974588@qq.com

† These authors have contributed equally to this work and share first authorship

RECEIVED 25 February 2023
ACCEPTED 21 March 2023
PUBLISHED 18 May 2023

CITATION
Bai T, Jiang Y, Yang J, Luo J and Du Y (2023) A data security scheme based on EEG characteristics for body area networks. *Front. Neurosci.* 17:1174096.
doi: 10.3389/fnins.2023.1174096

Body area network (BAN) is a body-centered network of wireless wearable devices. As the basic technology of telemedicine service, BAN has aroused an immense interest in academia and the industry and provides a new technical method to solve the problems that exist in the field of medicine. However, guaranteeing full proof security of BAN during practical applications has become a technical issue that hinders the further development of BAN technology. In this article, we propose a data encryption method based on electroencephalogram (EEG) characteristic values and linear feedback shift register (LFSR) to solve the problem of data security in BAN. First, the characteristics of human EEG signals were extracted based on the wavelet packet transform method and as the MD5 input data to ensure its randomness. Then, an LFSR stream key generator was adopted. The 128-bit initial key obtained through the message-digest algorithm 5 (MD5) was used to generate the stream key for BAN data encryption. Finally, the effectiveness of the proposed security scheme was verified by various experimental evaluations. The experimental results showed that the correlation coefficient of data before and after encryption was very low, and it was difficult for the attacker to obtain the statistical features of the plaintext. Therefore, the EEG-based security scheme proposed in this article presents the advantages of high randomness and low computational complexity for BAN systems.

KEYWORDS

body area network, electroencephalogram, data security, wavelet packet transform, linear feedback shift register

1. Introduction

Body area network (BAN) is an important means to solve problems, such as insufficient medical resources, rising treatment costs, and poor medical conditions, which are caused by the growing population in the world (Hassan et al., 2017; Abidi et al., 2020; Liu et al., 2021). As an emerging technology, BAN has aroused an immense interest in academia and industry since its inception. In 2012, the Institute of Electrical and Electronics Engineers (IEEE) published an official standard, IEEE 802.15.6: Wireless Body Area Networks (Standard, 2012). As shown in Figure 1, the said standard defines a human-centered wireless communication network as consisting of sensor nodes and related devices placed on or inside the human body (Pandey et al., 2019). Due to the particularity of BAN, the network transmits users' privacy information, and consequently, any unauthorized access or illegal data tampering will cause major problems to users; therefore, BAN has set high requirements for security (Shen et al., 2018; Hajar et al., 2021). However, the BAN system is limited in resources

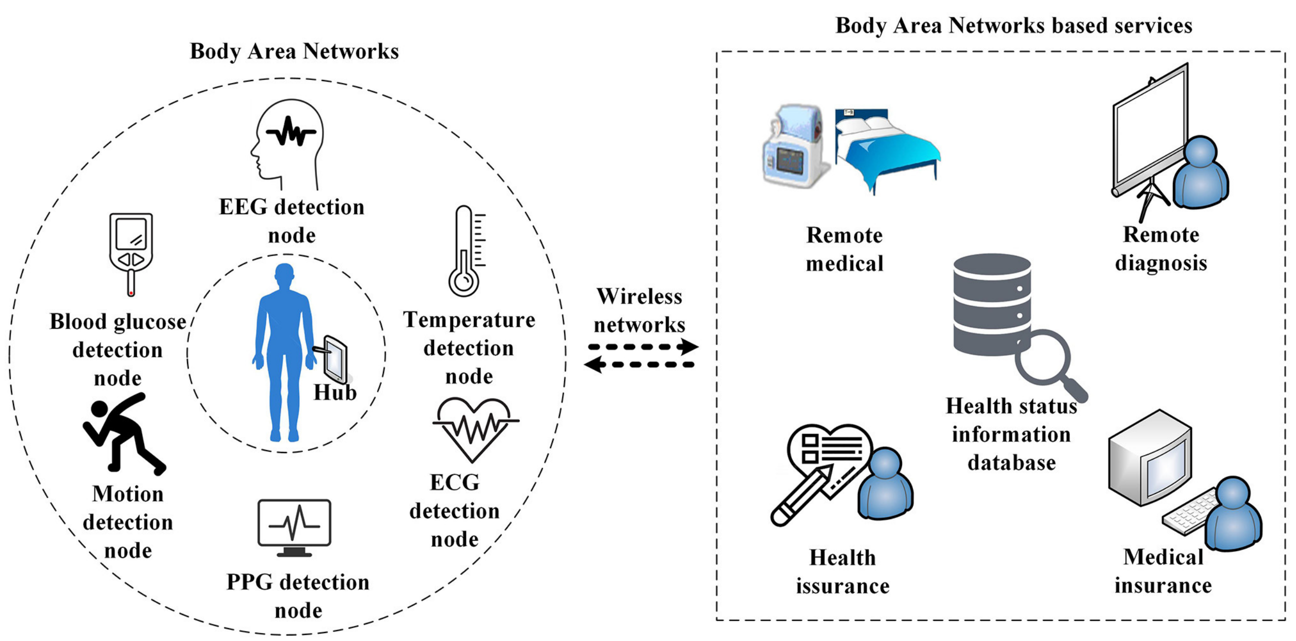

FIGURE 1
Body area network (BAN) system and its applications.

and is sensitive to the energy consumption of sensor nodes; therefore, most of the existing network security schemes are not applicable (Shi et al., 2012; Qadri et al., 2020). Therefore, designing a security solution with low power consumption and high-intensity security that meets the requirements of a BAN system to realize that data security has become a major challenge in the field of BAN research (Narwal and Mohapatra, 2021).

Researchers have proposed a variety of ways to improve the safety of BAN data. The first way for data encryption is the conventional symmetric encryption scheme. The advanced encryption standard (AES)-based encryption method for BAN data has been proposed in the study of Gangadari and Rafi Ahamed (2016). The second-order reversible one-dimensional cellular automata are used to replace the lookup tables in the AES algorithm to generate an S-box for the nonlinear substitution of data. The experimental results have shown that this scheme includes better security features than the conventional AES algorithm. However, generating the encryption key requires adequate amounts computation, and the BAN system uses more energy due to data encryption. Therefore, the conventional symmetric encryption scheme is not suitable for a BAN system (Bai et al., 2019; Wang et al., 2020). The second way for data encryption is based on the physiological sign information in a BAN system. Different from common sensor nodes, the sensor nodes in BAN collect human physiological sign parameters. These parameters will present different characteristics according to different individuals. Even for the same individual, the information on physiological signs is time-varying. Therefore, these parameters collected from the human body can be used for data security in a BAN system (Al-Janabi et al., 2017). Compared with traditional data encryption schemes, these key generation methods can effectively reduce energy consumption in the process of encryption (Liu et al., 2013; Mainanwal et al., 2015). In their study Wang et al. (2011) proposed a method to extract characteristic values of electrocardiogram (ECG) signals based on the implicit Markov model, and the encryption key for BAN data was generated by combining the hash function. This scheme does not require key distribution and strict time synchronization. Fast Fourier Transform (FFT) is performed on an ECG signal and photoplethysmogram (PPG) signal, respectively, as described in the study by Venkatasubramanian et al. (2008) and by Ramli et al. (2013), and the generated characteristic values and fuzzy algorithm are used to construct a security mechanism for BAN. In his study, Moosavi (2021) puts forward two different key generation methods based on the PPG signal to improve the security of BAN. The first method is realized using the Galois linear feedback shift register (LFSR) and a continuous interbeat interval (IBI) of the PPG signal. The second method is realized using the IBI as the seed generator for the AES algorithm. Compared with the existing methods that only rely on the IBI sequence, this method provides better random performance. In the study by Faragó et al. (2019), a time-domain technique based on the cross-correlation has been proposed to evaluate the characteristics of ECG, PPG, or electromyography (EMG) signals for the identification and authentication in BAN systems. This method can complete the security authentication of nodes without increasing the calculation amount of BAN nodes. In this article, we propose a security scheme based on the recognition of EEG characteristics and the LFSR method for BAN. The random EEG signal characteristics containing individual differences were calculated as the input data for MD5 to solve the security problem of the key. The simple structure of the LFSR was used to generate a random stream key, which improves the data encryption strength of a BAN system.

The remainder of this article is organized as follows: Section 2 puts forward the EEG signal and the characteristic value extraction method. Section 3 presents the initial key generation method based on MD5. Section 4 provides the generation method of keys based on the LFSR. Section 5 presents the experimental results of the encryption data and provides the analysis. Finally, the conclusion of the security scheme is given in Section 6.

2. EEG signal acquisition and characteristic value extraction method

2.1. EEG signal acquisition

Electroencephalogram (EEG) is a method for recording the effect of electrical activity on the nerve cells in the brain to reflect the brain activity in a human being. The human brain is made up of tens of thousands of neurons, and the EEG signals are the electrical signals that are generated by the activity between these neurons (Lotte et al., 2018). The single-lead EEG has poor determinacy and strong randomness, thus the nonlinear research is limited to some extent and the recognition results are poor. While the multi-lead EEG contains more information concerning the human brain, it can better re?ect the overall information on brain activity (Galderisi et al., 1996).

It is difficult to accurately characterize the electrical activity of the human brain because the EEG is characterized by a strong background noise, a weak signal amplitude, a strong non-stationarity, and randomness. The concept of frequency was first used to describe the electrical activity in the brain in 1929. The frequency of electrical activity in the human brain varies between 0.5 Hz and 30 Hz. At present, it is generally accepted that the range of EEG frequency variations is divided into four frequency bands, which are: (1) δ wave: frequency is 0.5–4 Hz and the amplitude is 20–200 μV. (2) θ wave: frequency is 4–7 Hz and the amplitude is 20–150 μV. (3) α wave: frequency is 8–13 Hz and the amplitude is 20∼100 μV. (4) β wave: frequency is 13–30 Hz and the amplitude is 5–20 μV.

In this study, the EEG experimental dataset SEED-IV was used for experimental testing. In SEED-IV, 15 volunteers between 20 and 24 years of age were involved in the experiment, and 72 movie clips were selected as a library of four emotions (happiness, sadness, fear, and neutral). Each volunteer was required to undergo three sessions with an interval of one week or more, and each session contained 24 trials. Each trial usually lasted ∼3 min and is divided into three parts: 5 s hint of start, approximately 2 min movie clip, and 45 s emotion assessment. In the dataset, EEG signals were extracted from each volunteer at different times during the same scene and the same stimulus. As shown in Figure 2, the multi-channel original EEG signals were extracted by the 62-channel ESI NeuroScan system with the sampling frequency of 200 Hz. The other irrelevant bands were filtered with filters ranging from 0.5 Hz to 75 Hz to remove noise. Then, the time-domain and frequency-domain characteristics of EEG signals were obtained, and the EEG signals were expressed effectively (Zhang et al., 2013; Meng et al., 2014; Yang et al., 2014).

2.2. Extraction method of EEG characteristics

Electroencephalogram is a time-varying and non-stationary signal. Since the EEG signal was discovered, the usual method of analysis is to calculate the power spectrum of the EEG signal by Fourier transform; however, the Fourier transform is based on the premise of a stationary random process. However, the EEG signals detected in practical applications cannot satisfy the hypothesis of stationarity, such as the EEG signals in sleep, seizure, or other states; therefore only by combining time and frequency processing can better results be obtained.

The wavelet transform is equivalent to a digital microscope, including the functions of magnification, narrowing, and panning. The function of a wavelet transform is similar to that of a set of band-pass filters with an equal bandwidth and a variable center frequency. Compared with the traditional Fourier transform, the wavelet transform is a local transform of space/time and frequency, which can effectively extract information from signals, and carry out a multi-scale detailed analysis of functions or signals through operational functions such as scaling and shift, with good time-frequency characteristics. The wavelet transform can provide a frequency-varying "time-frequency" window, which automatically narrows when high-frequency information is detected, allowing for a fine analysis of the signal at higher frequencies. When a low-frequency signal is detected, the "time-frequency" window is automatically widened to allow for conducting a profile analysis of the signal at a lower frequency. The time-frequency characteristics of the wavelet transform are very suitable for analyzing the transient characteristics and time-varying characteristics of non-stationary signals.

The wavelet packet decomposition, also known as optimal subband tree structuring, is the further optimization of the wavelet transform. The concept behind wavelet packet decomposition is to use the analysis tree to represent the wavelet packet, that is, to analyze the details of the input signal using the wavelet transform with several iterations. The idea behind the main algorithm of wavelet packet decomposition is that, on the basis of the wavelet transform, in each level of signal decomposition, in addition to the further decomposition of the low-frequency subband, further decomposition of the the high-frequency subband also takes place. Finally, by minimizing the cost function, the optimal signal decomposition path is calculated, and the original signal is decomposed according to the decomposition path. Compared with the traditional wavelet analysis, the wavelet packet analysis can adaptively select the best basis function according to the characteristics of the analyzed signal after the multi-level division of the frequency band so as to make it match the signal and improve the analysis ability of the signal (Yin et al., 2008). In the wavelet packet analysis, $\varphi(t)$

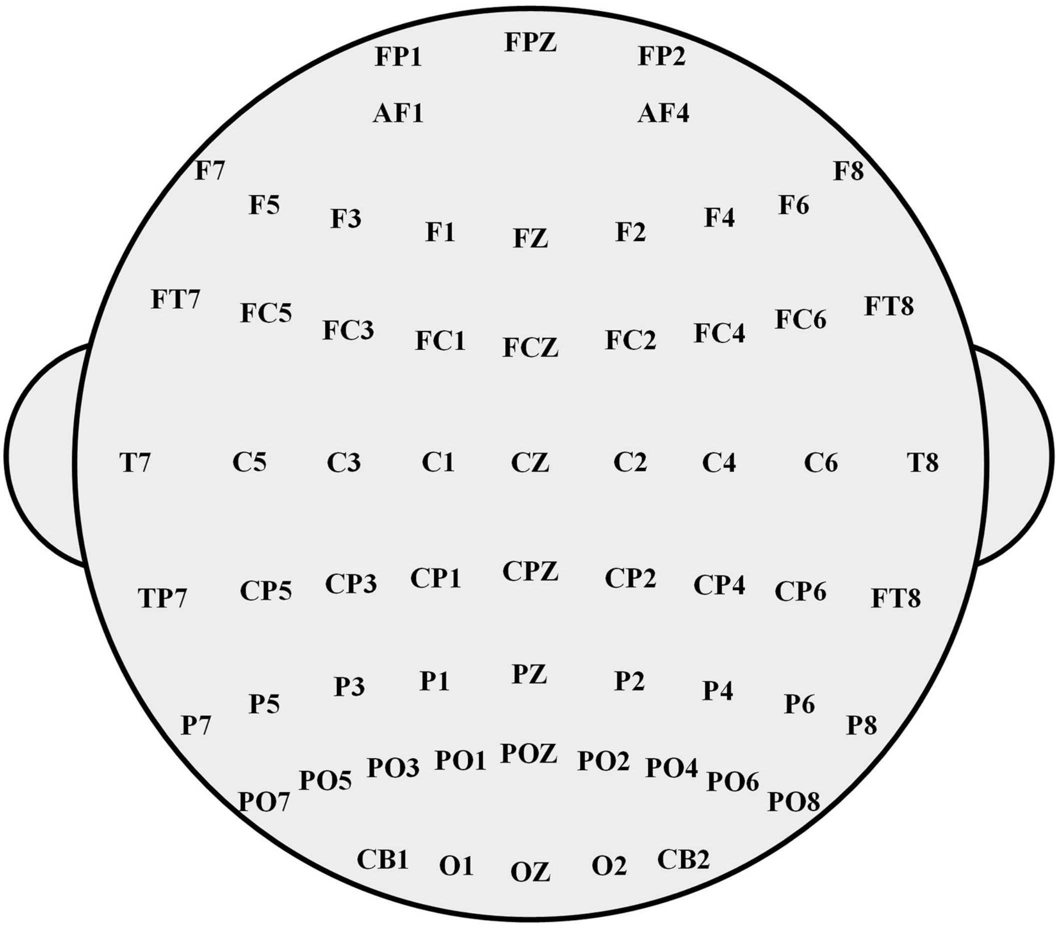

FIGURE 2
A 62-channel ESI NeuroScan system with the sampling frequency of 200 Hz.

represents the scale function and $\psi(t)$ represents the wavelet function, therefore:

$$\psi_0(t) = \varphi(t) \tag{1}$$

$$\psi_1(t) = \psi(t) \tag{2}$$

$$\psi_{2m}(t) = \sum_{k=-\infty}^{+\infty} h_k \psi_m(2t-k) \tag{3}$$

$$\psi_{2m+1}(t) = \sum_{k=-\infty}^{+\infty} g_k \psi_m(2t-k), \tag{4}$$

where h_k is the low-pass filter and g_k is the high-pass filter. Function $\{\psi_n\}$ is the wavelet packet of the scale function $\varphi(t)$.

In this article, the wavelet packet transform theory was used to process EEG signals, and the characteristics of different EEG frequency bands (α wave, β wave, δ wave, and θ wave) were calculated. Through a multi-resolution decomposition of the wavelet packet, the optimal wavelet packet tree was selected to reconstruct the specified EEG frequency bands. In this article, a discrete Meyer wavelet was used to decompose EEG signals. The Fourier transform of the Meyer wavelet scale function is:

$$\varphi(t) \begin{cases} (2\pi)^{\frac{1}{2}} & |t| < \frac{2\pi}{3} \\ (2\pi)^{-\frac{1}{2}} \cos\left[\frac{\pi}{2} \nu\left(\frac{3}{2\pi}|t| - 1\right)\right] & \frac{2\pi}{3} \leq |t| \leq \frac{4\pi}{3} \\ 0 & \text{else} \end{cases} \tag{5}$$

$$\nu(t) = \begin{cases} 0 & t \leq 0 \\ 1 & t \geq 1 \end{cases} \tag{6}$$

$$\nu(t) + \nu(1-t) = 1 \tag{7}$$

The EEG signal was decomposed into eight layers, and the minimum frequency resolution can be estimated by formula (8).

$$f_{\min} = \frac{f_s}{2 \cdot 2^8} = 0.3906\text{Hz}, \tag{8}$$

where f_s is the sampling frequency of the EEG signal and the value of f_s is 200 Hz.

The more the layers of wavelet packet decomposition, the higher the frequency resolution. The wavelet packet decomposition satisfies four kinds of EEG frequency band filtering requirements.

3. Initial key generation method

After performing the extraction method of EEG characteristics, MD5 and LFSR were used to generate keys for data encryption, as shown in Figure 3. The message-digest (MD) algorithm is a widely used password hash function, which has the following characteristics: first, the length of the output sequence calculated by the MD algorithm is fixed, regardless of the length of the input message. Second, the message digest appears randomly. In fact, different input data in the MD algorithm will result in different output sequences after calculation. Third, as the MD algorithm is a one-way function, it can only calculate the summary sequence from the input data bit can neither recover any input data from the output sequence nor find any information related to the input data from the output sequence. The MD5 algorithm generates a 128-bit (16-byte) hash sequence based on the input data. It can be used to verify the integrity and consistency of data transmission. The MD5 algorithm was announced in 1992 to replace the MD4 algorithm. MD5 treats the entire file as one large text message and generates a unique MD5 message digest through an irreversible string conversion algorithm. If anyone makes any changes to a file, its MD5 value will change.

The principle of the MD5 algorithm is that the input data was grouped into 512 bits. Each group was then divided into sixteen 32-bit subgroups, and the grouped data were processed through a series of calculations. Finally, the 128-bit hash output sequence is composed of four groups of 32-bit sequences in sequence. Figure 4 shows the process of the MD5 algorithm. Each operation was performed by the 128-bit result value of the previous round and the current 512-bit value. The MD5 process is as follows:

(1) In the MD5 algorithm, the input data need to be padded by bits first, and the bit number of the data modulo 512 is required to be 448. Even if the bit number of the input data modulo 512 yields exactly 448, it must be padded by bits. The first bit of the padding bits is 1 and the rest is 0.

(2) The MD5 algorithm uses four 32-bit registers, A, B, C, and D, to store intermediate variables and the final result. Registers A, B, C, and D are assigned initial values at the beginning of the MD5 calculation.

(3) MD5 algorithm defines four nonlinear functions, F, G, H, and I, to process the input data after grouping. Four different functions, F, G, H, and I, are used to process each 512-bit dataset. Each round takes the data in the updated register, A, B, C, and D, and the current 512-bit dataset as input and gets the new register values of A, B, C, and D after calculation.

(4) The final values of A, B, C, and D are spliced together in the order from low-bit data to high-bit data to form the output data.

4. Stream key generation based in LFSR

Taking some sequences existing in the shift register as the input of the linear feedback function, after making certain calculations in the function, the output results were filled to the leftmost end of the shift register so that such a shift register would have a continuous output. This shift register is called the linear feedback shift register (LFSR). In fact, the feedback function in the LFSR only performs an XOR on certain bits in the shift register and populates the result to the leftmost end of the shift register, as shown in Figure 5. The data of each bit in the LFSR may or may not participate in the XOR, and the bits that participate in the XOR are called taps. An *n*-order LFSR can only traverse 2^n-1 states at most, that is to say, the maximum period of an LFSR is 2^n-1. The sequence generated by an LFSR with a period of 2^n-1 is called the *m* sequence, and the *m* sequence has a higher encryption strength among the LFSR of the same level. The cipher text is calculated by the pseudorandom sequence XOR the plaintext.

The expression of the 128-order *m* sequence used for key generation is shown in formula (9).

$$f(N) = N^{127} + N^{126} + 1 \tag{9}$$

5. Experimental results and analysis

To verify the designed data security scheme based on EEG characteristics and LFSR, MATLAB software is used to simulate the encryption of image data. Using image data for verification of the designed data security scheme is important because the BAN system contains a large number of images such as electromyography images, endoscopic images, and medical images. Furthermore, image data are more intuitive for verification. In this article, the image Airplane and a medical endoscopic image were used to verify the encryption effect of the proposed data security scheme. Figure 6 shows the original images and the encrypted images.

Gray distribution refers to the distribution of gray value of gray images, which reflects the most basic statistical characteristics of an image and is generally represented by a gray histogram. The gray value distribution of the original image is usually uneven; therefore, there is a certain probability to crack the image data by calculating the statistical features. Figure 7 presents the gray histogram results of the image Airplane and the medical endoscopic image. As shown in Figure 7A, the left gray histogram is the gray value distribution of the original image, and it is relatively concentrated. However, after the encryption is completed, the result of the distribution of the images becomes more uniform, as shown in the right gray histogram of Figure 7A. Similar to Figures 7A, B yields the same result after encryption. Therefore, through the security scheme proposed in this article, the gray value distribution of the images is scrambled and became more uniform.

The two-dimensional correlation of images is used to verify the correlation degree of the original image data and the encrypted one,

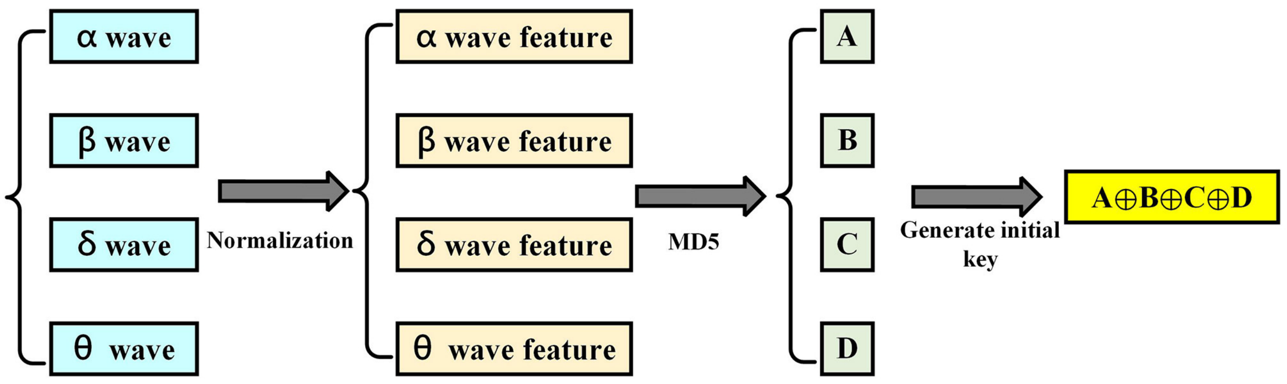

FIGURE 3
Flowchart of the key for BAN data security.

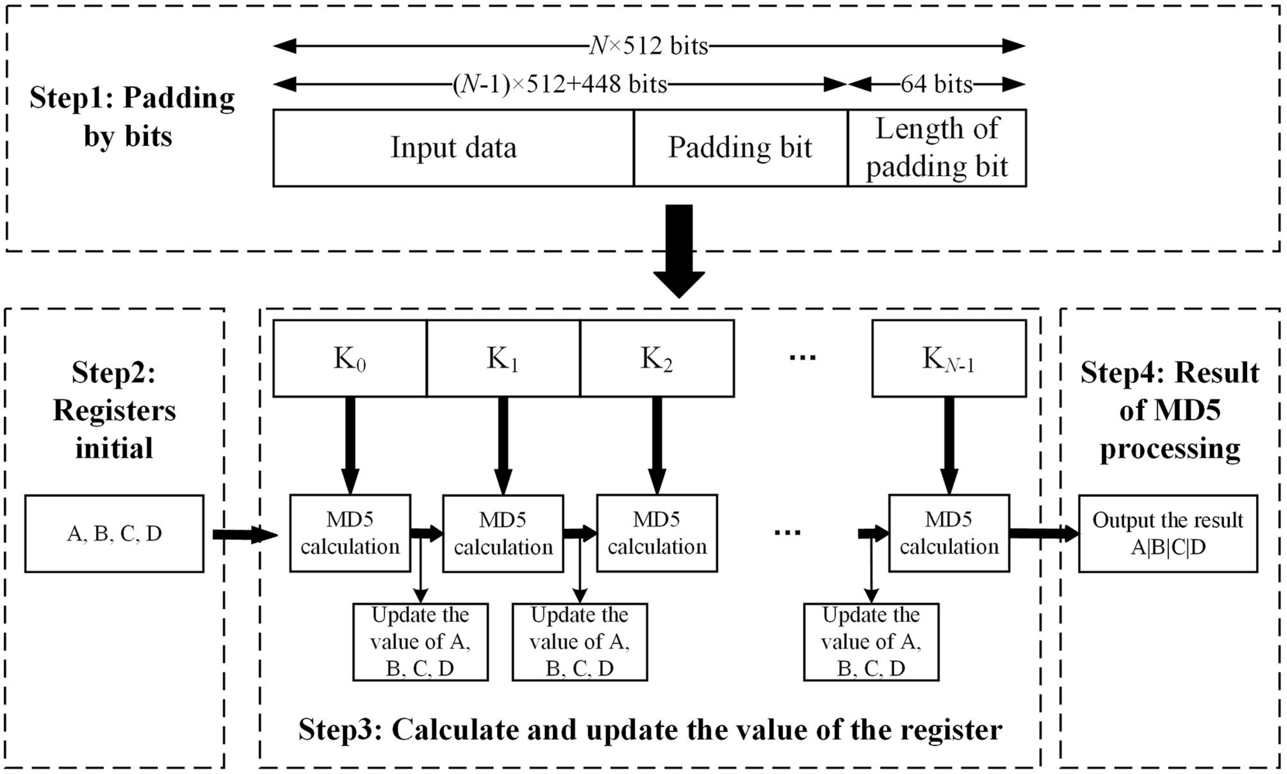

FIGURE 4
Flowchart of MD5 processing.

and K is the correlation coefficient. The calculation method of K is given as follows:

$$K = \sum_{a=1}^{M}\sum_{b=1}^{N}(O_{ab} - \overline{O})(E_{ab} - \overline{E}) / \sqrt{\left(\sum_{a=1}^{M}\sum_{b=1}^{N}(O_{ab} - \overline{O})^2\right)\left(\sum_{a=1}^{M}\sum_{b=1}^{N}(E_{ab} - \overline{E})^2\right)} \quad (10)$$

where O_{ab} and E_{ab}, respectively, represent the gray values of the image Airplane and the medical endoscopic image at the point (a, b) before and after the encryption.

After the designed method in this article was used to encrypt the image Airplane and the medical endoscopic image, the two-dimensional correlation coefficients K_1 $=1.38\times10^{-8}$ and K_1 $=3.24\times10^{-9}$ of the two images before and after encryption were calculated by formula (9). It can be observed that the two-dimensional correlation coefficient approaches 0,

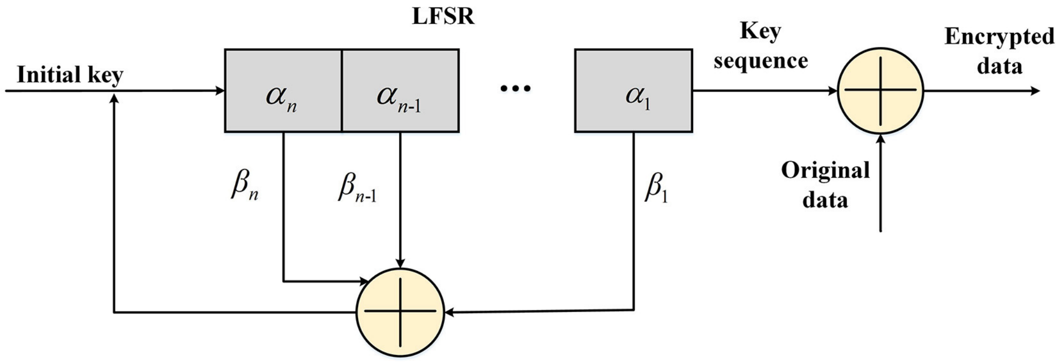

FIGURE 5
Linear feedback shift register (LFSR)-based encryption process.

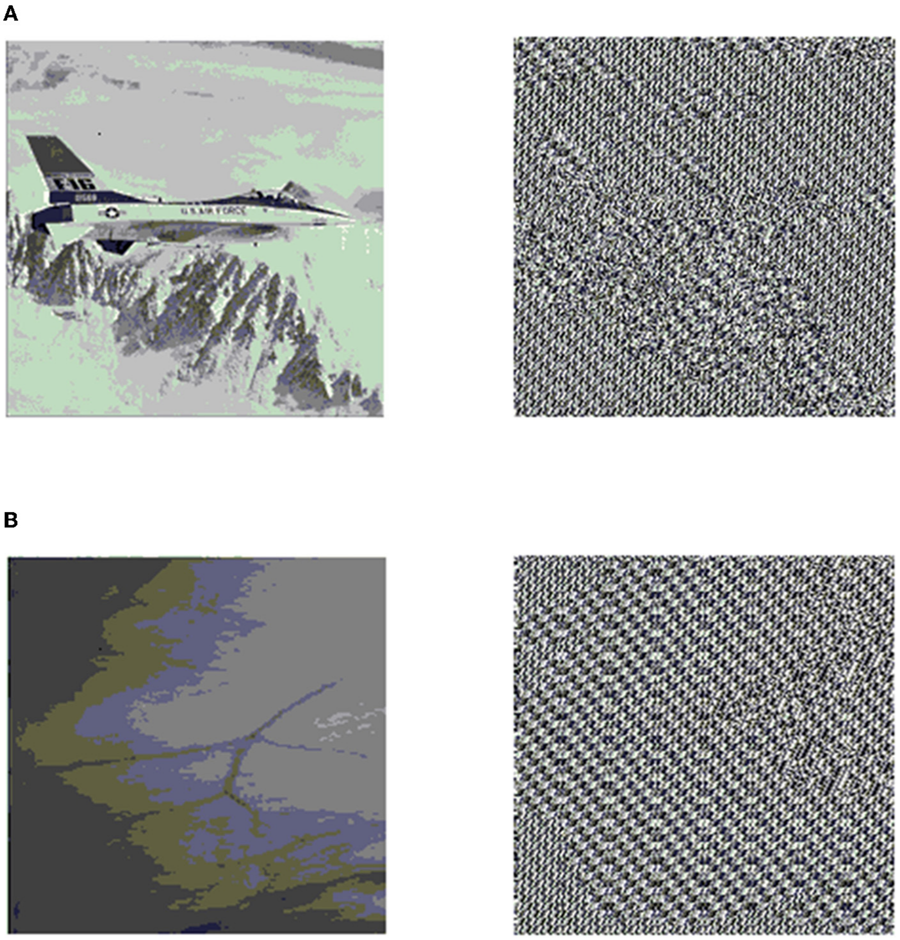

FIGURE 6
Original and encrypted images. **(A)** Airplane. **(B)** Medical endoscopic image.

indicating that the correlation of images before and after encryption is very low. This method can effectively encrypt image data.

To verify the correlation of adjacent pixels in the images, we select the adjacent pixel pairs in the original image and the encrypted one, and R is the correlation coefficient.

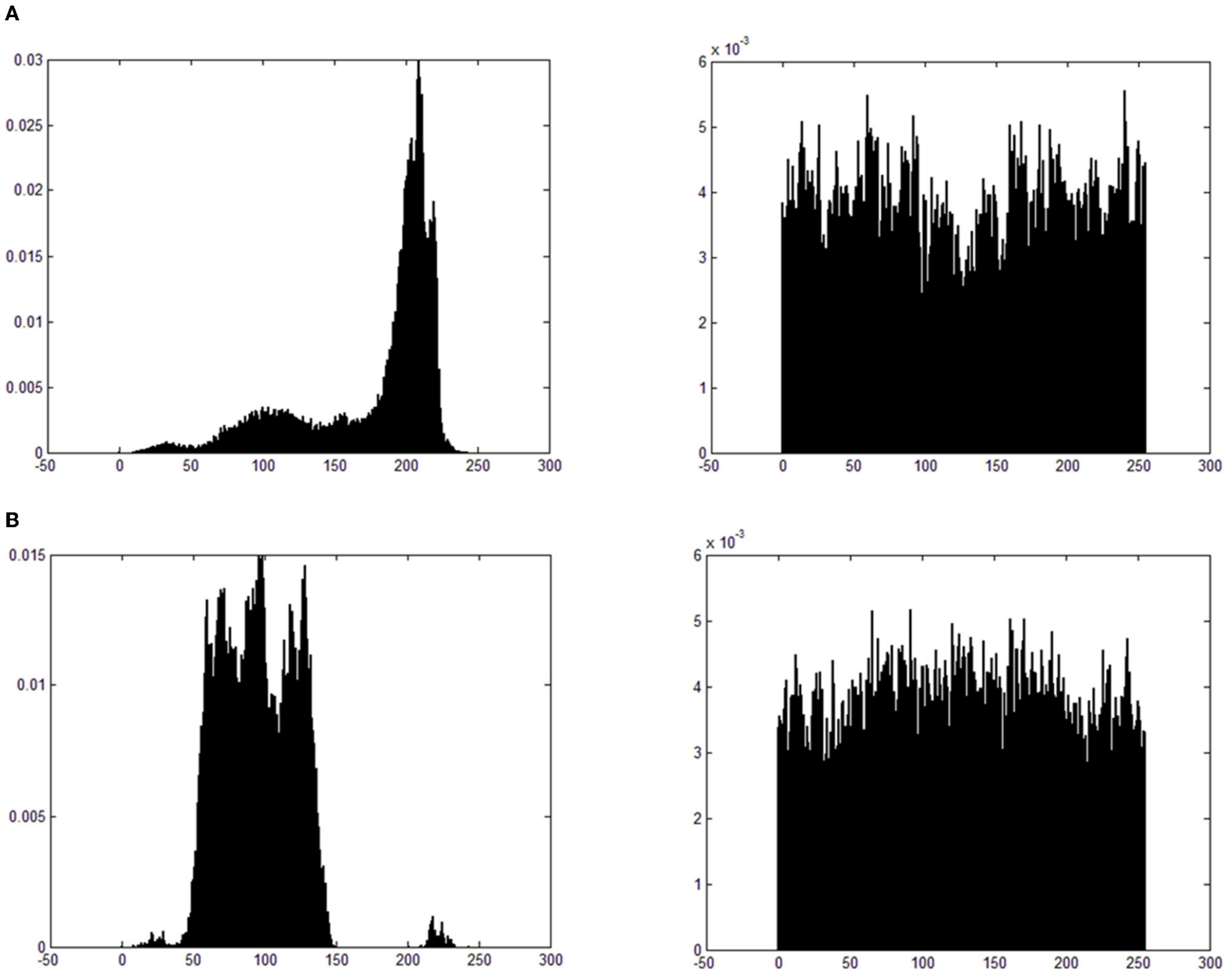

FIGURE 7
Gray histogram of the original and encrypted images. **(A)** Airplane. **(B)** Medical endoscopic image.

The calculation method of R is shown in formula (14). Furthermore, the correlation coefficients in the vertical, horizontal, and diagonal directions of the images are calculated, respectively,

$$E\left(x\right)=\sum_{i=1}^{N}x_i/N \tag{11}$$

$$D\left(x\right)=\sum_{i=1}^{N}\left[x_i-E\left(x\right)\right]/N \tag{12}$$

$$\operatorname{cov}\left(x,y\right)=\sum_{i=1}^{N}\left[x_i-E\left(x\right)\right]\left[y_i-E\left(y\right)\right]/N \tag{13}$$

$$R=\frac{\operatorname{cov}\left(x,y\right)}{\sqrt{D\left(x\right)D\left(y\right)}} \tag{14}$$

,

where x_i and y_i are the gray values of the ith adjacent pixel pairs, $E(x)$ and $E(y)$ are the averages of the image data, $D(x)$ and $D(y)$ are the variances, which measure the deviation between the image data and its average and N is the adjacent pair number of the image.

The calculated results of the correlation coefficient between the original image and the encrypted image are shown in Table 1. It is worth noting that, after data encryption of the image Airplane and the medical endoscopic image, the correlation of adjacent pixels in the three directions is effectively reduced, and it is difficult for the attacker to obtain the statistical features of the plaintext, thus improving the security of the system.

6. Conclusion

To meet the requirements of low power consumption and high-intensity security in a BAN system, this article proposes a data security scheme that is based on EEG characteristic values and LFSR construction. To be specific, the characteristics of EEG signals are mined by the wavelet packet transform, and α, β, δ, and θ waves are constructed to effectively characterize the features of EEG signals, which are input into the MD5 system through

TABLE 1 The correlation coefficient of the images in three directions.

Image name	*R*	Vertical direction	Horizontal direction	Diagonal direction
Airplane	Original	0.8834	0.9251	0.9118
	Encrypted	0.6247	0.2763	0.5570
Medical endoscopic image	Original	0.9251	0.9472	0.9346
	Encrypted	0.5896	0.3107	0.5713

normalization, and the initial key is calculated. Then, a 128-order *m* sequence is used to generate a stream key to encrypt privacy data in BAN. Finally, a variety of evaluation results prove that the proposed security scheme has enough ability to ensure data security in BAN. The BAN security scheme in this article only considers the method of data encryption; however, it does not consider the scheme of node authentication, which has certain limitations. In the future study, this project will invest more research in the following aspects. According to the relatively simple hardware structure of LFSR (m sequence), the advantages of the proposed method are further verified. Based on the characteristics of the BAN system, other types of feature extraction and calculation methods, such as ECG, PPG, and gait, will be studied to determine whether they are suitable for data security. There are still some important security problems in BAN that need to be solved. Therefore, the solutions for authentication with low power consumption and high reliability in BAN systems will be investigated by us.

Data availability statement

Publicly available datasets were analyzed in this study. This data can be found at: https://bcmi.sjtu.edu.cn/home/seed/seed-iv.html.

Author contributions

TB: conceptualization, methodology, writing—original draft, and writing—review and editing. JL: design of the methodology and validation of the experiments. YJ: validation and editing. JY: supervision. YD: validation. All authors contributed to the article and approved the submitted version.

Funding

The project was funded by the National Natural Science Foundation of China (62171073, 61971079, and U21A20447), the Department of Science and Technology of Sichuan Province (2020YFQ0025 and 2020YJ0151), the Project of Central Nervous System Drug Key Laboratory of Sichuan Province (210022-01SZ, 200020-01SZ, 200028-01SZ, and 200027-01SZ), the Nature Science Foundation of Chongqing (cstc2019jcyj-msxmX0275, cstc2020jcyj-cxttX0002, cstc2019jcyjmsxmX0666, cstc2021jscx-gksbx0051, and cstc2021jcyj-bsh0221), the Science and Technology Research Project of Chongqing Municipal Education Commission (KJZD-k202000604, KJQN202100602, KJQN202100602, and KJQN202000604), the Key Research Project of Southwest Medical University (2021ZKZD019), the special support for the Chongqing Postdoctoral Research Project (2021XM3010 and 2021XM2051), and the Project funded by the China Postdoctoral Science Foundation (2022MD713702, 2021MD703941, and 2021M693931).

Acknowledgments

We acknowledge the School of Optoelectronic Engineering of Chongqing University of Posts and Telecommunications for their assistance in the research.

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.

References

Abidi, B., Jilbab, A., and Mohamed, E. H. (2020). Wireless body area networks: a comprehensive survey. *J. Med. Engin. Technol.* 44, 97–107. doi: 10.1080/030920201729882

Al-Janabi, S., Al-Shourbaji, I., Shojafar, M., and Shamshirband, S. (2017). Survey of main challenges (security and privacy) in wireless body area networks for healthcare applications. *Egypt. Inform. J.* 18, 113–122. doi: 10.1016/j.eij.11001

Bai, T., Lin, J., Li, G., Wang, H., Ran, P., Li, Z., et al. (2019). A lightweight method of data encryption in BANs using electrocardiogram signal. *Fut. Gen. Comp. Sys.* 92, 800–811. doi: 10.1016/j.future.01031

Faragó, P., Groza, R., Ivanciu, L., and Hintea, S. (2019). A correlation-based biometric identification technique for ECG, PPG and EMG. In *2019 42nd international conference on telecommunications and signal processing (TSP)* (pp. 716–719). IEEE. doi: 10.1109./TSP.2019.8768810

Galderisi, S., Mucci, A., Bucci, P., Mignone, M. L., and Maj, M. (1996). Multilead quantitative EEG profile of clozapine in resting and vigilance-controlled conditions. *Psychiatry Res. Neuroimag.* 67, 113–122. doi: 10.1016./0925-4927(96)02883-1

Gangadari, B. R., and Rafi Ahamed, S. (2016). Design of cryptographically secure AES like S-Box using second-order reversible cellular automata for wireless body area network applications. *Healthcare Technol. Lett.* 3, 177–183. doi: 10.1049./htl.2016.0033

Hajar, M. S., Al-Kadri, M. O., and Kalutarage, H. K. (2021). A survey on wireless body area networks: architecture, security challenges and research opportunities. *Comp. Sec.* 104, 1–27. doi: 10.1016./j.cose.2021.102211

Hassan, M. M., Lin, K., Yue, X., and Wan, J. (2017). A multimedia healthcare data sharing approach through cloud-based body area network. *Future Gen. Comp. Sys.* 66, 48–58. doi: 10.1016/j.future.12016

Liu, J., Zhang, Z., Chen, X., and Kwak, K. S. (2013). Certificateless remote anonymous authentication schemes for wirelessbody area networks. *IEEE Transact. Parall. Distrib. Sys.* 25, 332–342. doi: 10.1109./TPDS.2013.145

Liu, Q., Mkongwa, K. G., and Zhang, C. (2021). Performance issues in wireless body area networks for the healthcare application: a survey and future prospects. *SN Appl. Sci.* 3, 1–19. doi: 10.1007./s42452-020-04058-2

Lotte, F., Bougrain, L., Cichocki, A., Clerc, M., Congedo, M., Rakotomamonjy, A., et al. (2018). A review of classification algorithms for EEG-based brain–computer interfaces: a 10 year update. *J. Neural Eng.* 15, 031005. doi: 10.1088./1741-2560/4/2/R01

Mainanwal, V., Gupta, M., and Upadhayay, S. K. (2015). A survey on wireless body area network: Security technology and its design methodology issue. In *2015 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS)* (pp. 1-5). IEEE. doi: 10.1109./ICIIECS.2015.7193088

Meng, J., Yao, L., Sheng, X., Zhang, D., and Zhu, X. (2014). Simultaneously optimizing spatial spectral features based on mutual information for EEG classification. *IEEE Transact. Biomed. Engin.* 62, 227–240. doi: 10.1109./TBME.2014.2345458

Moosavi, S. R. (2021). PPG-KeyGen: using photoplethysmogram for key generation in wearable devices. *Procedia Comput. Sci.* 184, 291–298.doi: 10.1016/j.procs.03038

Narwal, B., and Mohapatra, A. K. (2021). A survey on security and authentication in wireless body area networks. *J. Sys. Architect.* 113, 101883. doi: 10.1016./j.sysarc.2020.101883

Pandey, I., Dutta, H. S., and Banerjee, J. S. (2019). WBAN: a smart approach to next generation e-healthcare system. In *2019 3rd International Conference on Computing Methodologies and Communication (ICCMC)* (pp. 344-349). IEEE. doi: 10.1109./ICCMC.2019.8819713

Qadri, Y. A., Nauman, A., Zikria, Y. B., Vasilakos, A. V., and Kim, S. W. (2020). The future of healthcare internet of things: a survey of emerging technologies. *IEEE Commun. Surv. Tutorials* 22, 1121–1167. doi: 10.1109./COMST.2020.2973314

Ramli, S. N., Ahmad, R., and Abdollah, M. F. (2013). Electrocardiogram (ECG) signals as biometrics in securing wireless body area network. In *8th International Conference for Internet Technology and Secured Transactions (ICITST-2013)* (pp. 536-541). IEEE. doi: 10.1109./ICITST.2013.6750259

Shen, J., Gui, Z., Ji, S., Shen, J., Tan, H., Tang, Y., et al. (2018). Cloud-aided lightweight certificateless authentication protocol with anonymity for wireless body area networks. *J. Network Comp. Appl.* 106, 117–123. doi: 10.1016/j.jnca.01003

Shi, L., Li, M., Yu, S., and Yuan, J. (2012). *BANA: Body area network authentication exploiting channel characteristics. In Proceedings of the fifth ACM conference on Security and Privacy in Wireless and Mobile Networks* (pp. 27–38). doi: 10.1109./JSAC.2013.130913

Standard, I. E. E. E. for Local and metropolitan area networks part 15.6: Wireless Body Area Networks. *IEEE Std*. (2012) 802, 6. doi: 10.1109/IEEESTD.2012.6161600

Venkatasubramanian, K. K., Banerjee, A., and Gupta, S. K. (2008). "Plethysmogram-based secure inter-sensor communication in body area networks," in *MILCOM 2008-2008 IEEE Military Communications Conference* (pp. 1-7). IEEE. doi: 10.1109./MILCOM.2008.4753199

Wang, H., Fang, H., Xing, L., and Chen, M. (2011). An integrated biometric-based security framework using wavelet-domain HMM in wireless body area networks (WBAN). In *2011 IEEE international conference on communications (ICC)* (pp. 1-5). IEEE. doi: 10.1109./icc.2011.5962757

Wang, J., Han, K., Fan, S., Zhang, Y., Tan, H., Jeon, G., et al. (2020). A logistic mapping-based encryption scheme for Wireless Body Area Networks. *Future Gen. Comp. Sys.* 110, 57–67. doi: 10.1016/j.future.04002

Yang, C., Deng, Z., Choi, K. S., Jiang, Y., and Wang, S. (2014). Transductive domain adaptive learning for epileptic electroencephalogram recognition. *Artif. Intell. Med.* 62, 165–177. doi: 10.1016/j.artmed.10002

Yin, Y., Yu, H., and Zhang, H. (2008). A feature extraction method based on wavelet packet analysis for discrimination of Chinese vinegars using a gas sensors array. *Sens. Actuat. B Chem.* 134, 1005–1009. doi: 10.1016/j.snb.07018

Zhang, Y., Zhou, G., Jin, J., Wang, M., Wang, X., Cichocki, A., et al. (2013). L1-regularized multiway canonical correlation analysis for SSVEP-based BCI. *IEEE Transact. Neural Sys. Rehabilit. Engin.* 21, 887–896. doi: 10.1109/TNSRE.2013.2279680