Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 26 (2023), No. 7, pp. 1865–1873
DOI : 10.47974/JDMSC-1676

Cerebral disorders diagnosis via a secure transmission of multichannel EEG signal based on IoMT

Jamal A. Hammad *
College of Pharmacy
University of Anbar
Anbar
Iraq

Assef Raad Hmeed †
Department of Students Affairs and Registration
University of Anbar
Anbar
Iraq

Ahmed J. Obaid §
Department of Computer Science
Faculty of Computer Science and Mathematics
University of Kufa
Najaf
Iraq

Abstract

Electroencephalogram (EEG) data require a wider storage device setup due to its constant brainwave intensity logs and biosignal parameter. Therefore, effective compression systems are utilized before sending these signals to a medical station such as hospitals and therapy centres or through mobile medical instruments as one of the Internet medical things (IoMT) tools for real-time surveillance and analysis by specialists and anywhere. Conventional compression techniques can improve storage efficiency and help quickly transfer medical data from one computer to another because of their limited size. In addition, the received EEG (MCh-EEG) data are processed using various filtering methods to remove undesired noise and then compressed. The proposed method, which utilized buffer blocks, which is quite new in this field, was proposed. The smooth and safe transmission process

* *E-mail:* jamal.ali@uoanbar.edu.iq (Corresponding Author)
† *E-mail:* assef.raad@uoanbar.edu.iq
§ *E-mail:* ahmedj.aljanaby@uokufa.edu.iq

© Taru Publications

of multichannel EEG signals from the sensor to the surveillance is achieved by using highly effective methods to detect brainwaves, remove noise, compress and encrypt those signals. This work utilizes the mode of AES 256 BCM, which is rarely utilized in embedded systems, proving to be very powerful and effective in information ciphering.

Based on the proposed system's PRD parameter, the findings come as 0.41% and CR as 0.35%, and it's better than the current schemes. Experimental findings demonstrate the effectiveness of the proposed systems on 10 different records of MCH-EEG signals from the CHB-MIT Scalp EEG dataset.

Subject Classification: *91G20, 93B17.*

Keywords: *Multichannel electroencephalogram (MCh-EEG), Block-cipher mode (BCM-Operation), Advanced encryption standard (AES), Internet of medical things (IoT).*

1. Introduction

Diseases related to the brain have become very popular globally because certain causes actively impact people's physical condition. Due to its significance in brain surveillance, the transmission of the MCH-EEG signal was investigated several times. MCH-EEG signals hold the electrical waves of brain functions.

The standard scalp EEG signals range from "10-100" μV measured by the scalp (31) and "10-20" mV measured by electrodes below the dura mater [1]. Advances in the medical and mobile sciences have decreased the scale of sensor instruments significantly. The size of the sensor equipment was substantially reduced by phone and portable devices. Portable MCH-EEG sensors receive the signals and send these signals to CCTV for further review immediately.

A sensor maintains the ability to transmit any bit of signal without a buffer to the CCTV; this is in conventional systems [2]. Several obstacles arise because of the incorrect transmission rate or low communication channel bandwidth. A continuous signal flow can usually lead to a rise in the large volume of data [3]. Consequently, the wrong transfer rate or low bandwidth channel connectivity greatly affects the data volume.

A constant flow of signals will typically lead to a dropout and severe loss of vital information. However, reducing redundancy by compressing MCH-EEG data is necessary for storage space optimization, and the time taken for data conversion causes stability decreases [4]. In addition, biomedical MCH-EEG signals contain confidential personal health data and patient identity features. They can be encrypted before mass media dissemination to avoid unintended entry by cyber assailant adversaries [5]. The survey is carried out to ensure that the constructed applications perform well to satisfy the testing requirements. The survey involves comparing and distributing MCH-EEG data compression

and converting various methods. The simple methods of communication could yield better results for data compression. The effect of this compression can be accomplished using techniques such as sampling, transformation, filters, amplifying, and code and using the wireless network. The results of the encoding and transmission are seen after the surveys.

2. Literature Research

This part includes a thorough discussion with many other machine learning classifiers and previous similar studies on functional extraction using linear and nonlinear approaches. Several methods for predicting epileptic seizures based on linear and nonlinear EEG signals have been published [6]. In the techniques proposed by these studies, function extraction strategies are required to distinguish between non-seizure, seizure, and normal EEG behaviour using machine learning algorithms. All included are sub-band frequency extraction, entropy analysis, wavelet degradation, highest exponentiation of Lyapunov, fractal estimation, Hearst power, and high cumulative order. Kumar and colleagues [7] Recently suggested ambiguous approximate entropy (fApEn) and an EEG-dependent WT extraction method.

According to Chen et al., studies have proposed a way to overcome the computing load of the classic wavelet transform. [8] Formal paraphrase ANNs and logistic regression were used to characterize the behaviour of epileptic seizures. Furthermore, epileptic events were categorized using artificial neural networks and logistic regression. Kumar and colleagues [9].

The fApEn approach was recently used to create an SVN for functional classification. The EEG was divided into subdomains of the umbilical wavelet shunt, and fApEN measured the troubled behaviour of the EEG signals for each subdomain. Using the SVN classifier, the authors and RBF achieved the greatest classification accuracy. According to a literature review, most seizure-free-EEG activity trials from stable EEG data failed to produce optimum results. EEG FeExt can also be used for classification, pattern recognition, and event detection poor analytical results from hand-designed EEG extraction procedures. The FeExt repeat auto-coding for EEG [10] method is then used. FxExt also improves the classification and grouping of the echo state grid. The b and l spatial tempo distributions classify "motor imaging." The accuracy and speed of graduated regression and recursive classification approaches are lower. Thus, the Perceptron Multilayer Neural Network (MLP-NN) performs EEG classification [11]. The velocity and precision of convergence are measured and compared to the metaheuristic algorithm's effectiveness. Neurocognitive ability is a person's emotional/cognitive ability used in neuroscience research. The recording of sleep points is the neurocognitive effect.

Using long-term memory blocks in the repetitive neural network [12] improves classification accuracy, including sleep marking, non-rapid eye movement, and the N1 stage during sleep, which denotes the transition between sleepiness and wakefulness. Deep learning is used to find temporal dependence in the EEG [13]. An LSTM [14] would be used to detect high-level patterns in

the EEG. With LSTM, stable epilepsy characteristics can be extracted with the help of a fully connected layer, and output labels can be extracted with the help of a Softmax layer. Furthermore, it is highly efficient at identifying devices such as eye and muscle movements, background noise in EEG recordings, etc. Identifying fixed-time features of the EEG and switching between sleep periods are among the biggest challenges.

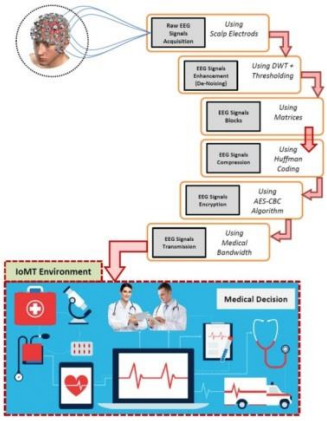

Figure 1
The System Methodology flowchart

3. Research Methodology

The compression and encoding block diagram of the recommended MCH-EEG method is seen in Figure 1. The biomedical MCH-EEG signal was loaded into the device in the initial step. The next step is noise reduction by using DWT and signal threshold penetration. The third step is to establish block MCH-EEG signals. A Huffman coding for any MCH-EEG signal block applies the compression technique next to the fourth step. The encryption mechanism was used based on the AES-BCM algorithm during the 5th stage after the completion of the previous step, and the MCH-EEG signal was handled in the transmission block. Finally, the decryption and decompression protocol prevents block aggregation after the reception of the MCH-EEG signal, relying on the AES-BCM inversion and the Huffman inversion coding to get the original MCH-EEG biomedical signal.

3.1 *Compressing*

Compressing is decreasing the data size of arithmetic procedures or systems. The compression ratio (CR) is used to evaluate the effectiveness of a given compression strategy and the level of data compression achieved. Both lossy and lossless compression models exist. When decompressed, the file would be restored to its pre-compression state in the loose scheme without losing any information [20]. Most of the time, the applications such as Medical

Health Records (MHR), files of financial reports, and other necessary files are continuously processed by a lossless system, as any single bit loss can also have an aversive effect. The various parameters such as PRD, CR and QS are utilized for compression performance assessments [18]. CR is the compression measure obtained by encoding mechanisms in the signal. It does not compress signal quality information but tests the algorithm's efficacy in reducing storage capacity. Therefore, to assess the error or variance between the original signal and the reconstructed signal called PRD. QS is utilized to determine the compression efficiency when ignoring the errors in signal reconstruction [11] [17].

3.2 *AES Algorithm*

In October 2000, AES awarded one of the algorithms that qualified for the NIST finalists, the most stable algorithm. It is also known as Rijndael. It is a 128-bit fixed, 128-bit, 192-bit or 256-bit variable [15]. It is also known as Rijndael. This symmetrical algorithm uses a hidden key for encrypting and decrypting all. Four primary steps exist during a round of AES encryption/decryption [14]. ShiftRows is the permutation step, whereas Substitution Byte, MixRows, and AddRoundKey [20] are the other three substitution stages. Figure 1 demonstrates the Advanced Encryption Protocol algorithm for encryption and decryption. The major tallness (Nk) is 8, i.e. 32-bit 8-words, 256-bit AES, 4, i.e. 32, 32, and 14, i.e. 4-words (Nr). The ciphering function [8]:

$$\text{Encryption}\ (\text{integer}[4 * \text{NB}], \text{out}[4 * \text{NB}], \text{W}(\text{Nr} + 1)]) \tag{4}$$

In the next stages, the purpose of ciphering can be elaborated: let st be the state and round be rd; both hardware and software work well for AES. Five operating modes are available for AES, e.g., "ECB," "BCM," "CFB", "OFB", and "CTR" [19].

4. Findings and Discussion

This part summarizes and shows the findings of this article. In this work, DWT utilized a clean MCH-EEG signal with a threshold. Compression MCH-EEG signal utilized a lossless approach HuffCd-based algorithm and encrypted the MCH-EEG signal with the AES-BCM Block Ciphering asymmetric key encryption. The tests conducted are achieved on a device with specifications (Intel Processor Core(TM) i7-4400U CPU@2.50GHz 2.49 GHz, 4GB RAM, competent 64-bit MATLAB under Windows 10) (R2018b). Some parameters were applied to examine the implementation of the proposed system, with the compression efficiency parameters for denoise signals MSE, PSNR, SNR, CC PRD and CR. They are critical metrics to evaluate the system performance suggested at the end of the timely implementation and protection stage. The computational time of the system model may thus be defined as the time used on the system[16]. The output metric includes the compression and

Table 1
Proposed System Execution Time (in Second)

Block's No.	Time for AES Key Generation	Compression Time	Encryption Time	Decryption Time	Decom-pression Time	System Process Total Time
Whole	0.1766	7.188	5.7334	5.5436	2.901	11.325
4	0.1766	5.322	5.3998	5.239	1.503	9.7456
8	0.1766	6.766	7.219	3.82	1.4990	8.222
16	0.1766	3.201	4.669	5.332	0.7869	17.3920
24	0.1766	3.618	11.3351	10.610	1.3334	10.1298
32	0.1766	4.933	8.0671	8.232	1.4381	18.2843
40	0.1766	7.419	14.71	10.543	0.5521	22.1398
46	0.1766	5.7021	14.992	12.554	0.309	25.1221
60	0.1766	6.2291	14.549	7.768	0.645	36.9856

encryption technique used by the ECG input signals before the devices are transmitted to a device and the time needed to compress and encrypt the computer. Consequently, the average duration of the decryption and decompression technique used for processing the receiving file was calculated after receiving the item, which is the computed decryption time and the calculation time used for the MCH-EEG signal. The execution time for key generation, encoding, encryption, decryption, decompression, and the overall proposed device time in the MCH-EEG signal input file, as shown in Table 1, is the execution time for key generation, encoding, encryption, decryption, decompression, and the overall proposed device time, respectively. Therefore, for the four MCH-EEG signal blocks, the time of execution is 3.2808, 3.8548, 3.5344, and 0.616 for each block in the second as illustrated in Figure (2).

Some parameters for de-noise signal MSE, PSNR, SNR, and CC were used to evaluate the suggested method's execution. PRD and CR are compression

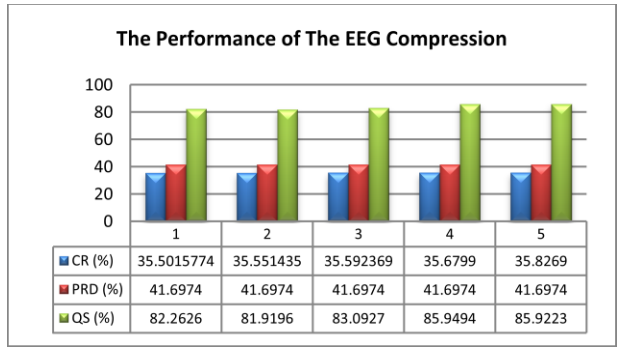

Figure 2
The Performance of The MCH-EEG Compression

performance parameters. Finally, timely execution and security are important factors when evaluating the suggested system's performance. As a result, the time consumed by each process in the system model may be characterized as the computing time of the system model. Two performance parameters are the computational compression and encryption time needed for processing the EEG signal before conversion to system monitoring. The findings demonstrate that the suggested system with four blocks takes less time to execute than alternative systems with more blocks.

Table 1 compared with other algorithms in previous analyses of the new compression algorithm. The HAAR wavelet denoise results range from 0.5 dB to 6 dB, as seen in Figure 2. PSNR is relatively high and the lowest on record no. 106 and 213. MCH-EEG signal compression attempts to attain a higher rate of compression without affecting the strength of the signal. CR should be tested using the other parameters to test the experimental results on the consistency of the reconstructed MCH-EEG signal.

5. Conclusion

This manuscript tries to propose a novel lightweight system design to effectively and safely process MCH-EEG signals. To examine the effectiveness of the recommended system, 5- separate important datasets from CHB-MIT Scalp EEG repository were processed within different mechanisms such as; denoising, filtering, compression, and encryption.

When time-critical data transmission is required, the delay efficiency of compression algorithms is especially significant. Compared to raw MCH-EEG signals, compressed signals require less time to calculate, so the Huffman lossless scheme is utilized. The efficacy of those processes is computed in terms of PRD, CR, SNR, PSNR, MSE, and QS. The PRD finding of the recommended work comes as 0.41 percent and CR as 0.35 percent, which is very better than existing schemes. The Experimental findings confirm that the algorithm's efficacy was utilized. The processing of the block level and signal encryption utilizing the 256-bit key algorithm AES-BCM could provide a higher level of security, which could be completely new to real-time integrated devices in this work to be examined.

References

[1] Abdulbaqi, A. S., Nejrs, S. M., Mahmood, S. D., & Panessai, I. Y. : A Tele Encephalopathy Diagnosis Based on EEG Signal Compression and Encryption. In International Conference on Advances in Cyber Security, pp. 148-166 (2020), December). Springer, Singapore.

[2] Dose, H., Møller, J. S., Iversen, H. K., & Puthusserypady, S. : An end-to-end deep learning approach to MI-EEG signal classification for BCIs. Expert Systems with Applications, 114, 532-542 (2018).

[3] Salazar-Gomez, A. F., DelPreto, J., Gil, S., Guenther, F. H., & Rus, D.: Correcting robot mistakes in real time using EEG signals. In 2017 IEEE International Conference on Robotics and Automation (ICRA), pp. 6570-6577 (2017, May). IEEE.

[4] Jain D.K., Dubey S.B., et al. : An approach for hyperspectral image classification by optimizing SVM using self-organizing map, *Journal of Computational Science* (2017).

[5] Zareapoor, M., Shamsolmoali, P. and Yang, J. : Kernelized Support Vector Machine with Deep learning: an Efficient Approach for extreme multiclass dataset, *Pattern Recognition Letters* (2017).

[6] K. Fu, J. Qu, Y. Chai, Y. Dong, Classification of seizure based on the time-frequency image of EEG signals using HHT and SVM, *Biomed. Signal Process. Control* 13, 15–22 (2014).

[7] S.-H. Lee, J.S. Lim, J.-K. Kim, J. Yang, Y. Lee, Classification of normal and epileptic seizure EEG signals using wavelet transform, phase-space reconstruction, and Euclidean distance, *Comput. Methods Programs Biomed*.116, 10–25 (2014).

[8] G. Chen, Automatic EEG seizure detection using dual-tree complex wavelet-Fourier features, *Expert Syst. Appl.* 41, 2391–2394 (2014).

[9] Y. Kumar, M. Dewal, R. Anand, Epileptic seizure detection using DWT based fuzzy approximate entropy and support vector machine, *Neurocomputing* 133, 271–279 (2014).

[10] Sun L, Jin B, Yang H, Tong J, Liu C, Xiong H : Unsupervised EEG feature extraction based on echo state network. Inf Sci 475:1-17 (2018).

[11] Afrakhteh S, Mosavi MR, Khishe M, Ayatollahi A : Accurate classification of EEG signals using neural networks trained by hybrid population-physic-based algorithm. *Int. J. Autom. Comput.* (2018). https://doi.org/10.1007/s11633-018-1158-3.

[12] Michielli N, Acharya UR, Molinari F : Cascaded LSTM recurrent neural network for automated sleep stage classification using single-channel EEG signals. *Comput Biol Med* 106 : 71–81 (2019).

[13] Hussein R, Palangi H, Ward RK, Wang ZJ :Optimized deep neural network architecture for robust detection of epileptic seizures using EEG signals. *Clin Neurophys* 130 : 25–37 (2018).

[14] Doborjeh MG, Wang GY, Kasabov NK : A spiking neural network methodology and system for learning and comparative analysis of EEG data from healthy versus addiction treated versus addiction not

treated subjects. In: IEEE transactions on biomedical engineering, pp 0018-9294 (2015).

[15] Doborjeh ZG, Doborjeh MG, Kasabov N : Attentional bias pattern recognition in spiking neural networks from spatiotemporal EEG data. *Cognit Comput* (2017). https://doi.org/10.1007/ s12559-017-9517-x.

[16] Hadjileontiadis, L. J. : Biosignals and compression standards. In M-Health, pp. 277-292 (2006). Springer, Boston, MA.

[17] Lee, S., Kim, J., & Lee, M. : A real-time ECG data compression and transmission algorithm for an e-health device. IEEE Transactions on Biomedical Engineering, 58(9), 2448-2455 (2011).

[18] Sriraam, N., & Eswaran, C. : Performance evaluation of neural network and linear predictors for near-lossless compression of EEG signals. IEEE Transactions on Information Technology in Biomedicine, 12(1), 87-93 (2008).

[19] Sriraam, N., & Eswaran, C. : An adaptive error modeling scheme for the lossless compression of EEG signals. IEEE Transactions on Information Technology in Biomedicine, 12(5), 587-594 (2008).

[20] Banerjee, A., Basu, K., & Chakraborty, A. : Prediction of EEG signal by digital filtering. In Proceedings of International Conference on Intelligent Systems & Networks, Jagadhri, India (2007).

[21] Azmi Shawkat Abdulbaqi, Ahmed J. Obaid & Maysaa Hameed Abdulameer. Smartphone-based ECG signals encryption for transmission and analyzing via IoMTs, *Journal of Discrete Mathematical Sciences and Cryptography* (2021), DOI: 10.1080/09720529.2021.1958996.

[22] Mohamad, R. : Data hiding by using AES Algorithm: Data hiding by using AES Algorithm. *Wasit Journal of Computer and Mathematics Sciences*, 1(4), 112-119 (2022).

[23] Azmi Shawkat Abdulbaqi, Ahmed J. Obaid & Alyaa Hashem Mohammed. ECG signals recruitment to implement a new technique for medical image encryption, *Journal of Discrete Mathematical Sciences and Cryptography*, 24:6, 1663-1673 (2021), DOI: 10.1080/09720529.2021.1884378.

[24] Abd Ali, D. M., Chalob, D. F., & Khudhair, A. B. : Networks Data Transfer Classification Based On Neural Networks. *Wasit Journal of Computer and Mathematics Sciences*, 1(4), 207-225 (2022).

Received October 2022