IIETA International Information and Engineering Technology Association
Advancing the World of Information and Engineering

Mathematical Modelling of Engineering Problems
Vol. 10, No. 6, December, 2023, pp. 2079-2085
Journal homepage: http://iieta.org/journals/mmep

A Secure Proposed Method for Real-Time Preserving Transmitted Biomedical Signals Based on Virtual Instruments

Azhar Kassem Flayeh[1], Bourair Al-Attar[2], Mohanad Sameer Jabbar[3], Lateef Abd Zaid Qudr[4], Jamal Fadhil Tawfeq[5], Poh Soon JosephNg[6*]

[1] Department of Electrical and Computer Engineering, Yildiz Techniqal University, Istanbul 34220, Turkey
[2] College of Medicine, University of Al-Ameed, Karbala 1238, Iraq
[3] Medical Instruments techniques Engineering Department, Technical College of Engineering, Al-Bayan university, Baghdad 10071, Iraq
[4] Department of Computer, Techniques Engineering, AlSafwa University College, Karbala 56001, Iraq
[5] Department of Medical Instrumentation Technical Engineering, Medical Technical College, Al-Farahidi University, Baghdad 00965, Iraq
[6] Faculty of Data Science and Information Technology, INTI International University, Persiaran Perdana BBN, Nilai 71800, Negeri Sembilan, Malaysia

Corresponding Author Email: joseph.ng@newinti.edu.my

Copyright: ©2023 IIETA. This article is published by IIETA and is licensed under the CC BY 4.0 license (http://creativecommons.org/licenses/by/4.0/).

https://doi.org/10.18280/mmep.100618

Received: 14 April 2023
Revised: 15 May 2023
Accepted: 21 May 2023
Available online: 21 December 2023

Keywords:
computer science, network, virtual instruments (LabVIEW), electrocardiogram (ECG), transform of discrete fourier series (DFT), inverse transform of discrete fourier series (IDFT)

ABSTRACT

Biomedical signals, encompassing electrocardiograms (ECG), electroencephalograms (EEG), electrooculograms (EOG), and other physiological data, are subjected to collection, preprocessing, and information extraction to discern patterns and trends. Given the transmission of these physiological activities over the Internet, the potential for unauthorized access necessitates stringent scrutiny. To mitigate data loss and theft, encryption of biomedical signals is implemented, with a particular emphasis on preserving the confidentiality of biomedical data. Commonly encrypted data include .dat signal files, images, confidential emails, user data, and directories. This paper proposes a robust method for encrypting and decrypting .dat files, specifically for ECG signals, utilizing the discrete fourier transform (DFT) and its inverse (IDFT). Through the use of LabVIEW software, the encryption module accepts the .dat input, converts it into ASCII values, and then performs DFT on them. The encrypted data is subsequently stored for transmission with the support of a security key. Data is decrypted using the security key and IDFT is applied. A transformation is performed so that the ASCII values are returned to the original string format. In addition to demonstrating enhanced security for signals and information transmitted over long distances, the proposed encryption method is also able to achieve significant savings in data transmission costs.

1. INTRODUCTION

Cybersecurity is a vital component of modern digital infrastructure due to the widespread implementation of encryption in numerous civilian systems. This is particularly true in covert communications. Based on a 2007 study by the Institute of Computer Security, 82% of businesses encrypt their data in transit, and 61% encrypt some stored data [1]. Files stored on computers or USB drives can be protected by encryption. A lot of sensitive information has been exposed due to misplaced or stolen backup disks and laptops in recent years.

Electronic devices for measuring the electrical output of humans, such as electrocardiograms (ECGs), electroencephalograms (EEGs), electromyograms (EMGs), and electrooculograms (EOGs), are available digitally [2]. In the event that physical security measures do not work, encrypting these files is an additional layer of security.

The military, the medical field, and science all use encryption for data in transit across networks. A full range of wireless devices are affected, including Bluetooth-enabled devices, mobile devices, wireless audio equipment, wireless intercom systems, and automated teller machines. Recent reports of data interceptions emphasize the significance of encryption. As health monitoring data is sensitive, it must be protected from unauthorized access. For health monitoring, traditional cryptographic methods often fall short due to their low efficiency and security limitations. The biometric authentication method can overcome these limitations by verifying an individual's innate characteristics [4].

A message's confidentiality can be ensured with encryption, but its integrity and authenticity cannot be protected independently, such as by message authentication codes (MACs) and digital signatures. There are several

cryptographic standards and software available. Nevertheless, encrypting data for security is a complex process. A single design or execution error can render attacks effective without necessarily disabling the encryption, potentially allowing an attacker access to unencrypted data [5]. This paper is organized as follows: The proposed methodology for data security utilizing cryptosystems is detailed first. This is followed by a comprehensive review of existing cryptography techniques. Subsequently, the results of the proposed technique and related attacks are discussed. A comparison is made between the proposed method and the literature available. The paper concludes with a summary of the findings and potential directions for future research.

2. LITERATURE REVIEW

One of the many articles that have been written about image steganography focuses on the security of embedded messages. In an ECG signal embedded with a binary watermark, Dey et al. [6] utilized a session-based blind watermarking technique, which degraded shape quality as the amplification factor increased. An approach based on wavelet steganography was utilized by Ibaida, and Khalil [7] and Chen et al. [8] to protect patient information. An ECG signal's amplitude was reduced utilizing a single-coefficient quantization and watermarking approach in one study, which combined DWT, DCT, and DFT. Watermarked ECG signals had deteriorating shape quality as quantization size increased. Large volumes of confidential ECG data can be effectively reduced for transmission utilizing signal compression technologies. A compression technique for ECG files proposed by Fira and Goras [9] combines Coding with LZW, filtering adaptively hysteretic and Extraction at local extremes based on the QS metric. Lee et al. [10], a data compression in real-time was described and transfer technique for a periodic ECG signal between e-health terminals. Compression ration (CR), the percentage root-mean-square difference (PRD), the normalized percentage root-mean-square difference (PRDN), the root mean square error (RMSE), The signal-to-noise ration (SNR), and the quality score (QS) values were utilized by the authors to demonstrate significant performance improvements. The CS signal acquisition/compression paradigm has been evaluated by Mamaghanian et al. [11] for the compression of ECG records utilizing Shimmer WBSN motes with low complexity and energy efficiency. When using WBSN-based ECG monitoring devices, as an alternative to DWT-based ECG compression, CS is a competitive alternative. An ECG data compression study also proposed DWT coefficient thresholding, Q-, R-, and S-wave estimations [12]. As a result, the compression ratios were higher with less distortion and efficiencies of computation than those obtained with earlier methods. Agulhari [13] utilized a wavelet-based compression technique to minimize compression distortion for each ECG. AFD and symbol substitution (SS) are utilized in Ma et al. [14] to compress ECGs for e-health applications. There were two phases to their compression. Lossy compression utilizing AFD was achieved first. A second improvement was made at the SS level to provide lossless compression and built-in data encryption. To choose the most sparse ECG representation, Adamo et al. [15] looked into a brand-new, effective signal compression approach. Their method relies on a series of fundamental building blocks extracted from the first transit of the signal. Sliding windows are used to collect successive blocks in order to promote sparsity. Comparing Elgendi et allossy.'s technique against other lossless/lossy ECG compression techniques, Elgendi et allossy.'s produced higher CRs and PRs. The DCT-based method can be used to compress ECG data in addition to two-encoding, according to Jha et al. [16]. A simple method Elgendi et al. described for compressing ECG signals in his paper [17] provides good compression while also providing good detection accuracy. One of the most critical factors in a patient's diagnosis and care is vital to sign information, which includes blood pressure, temperature, respiration rate, and heart rate since it allows physicians and other healthcare professionals to decide on the appropriate treatment options and well-being of a patient [18, 19]. Blood pressure and temperature are typically measured once every few hours in the intensive care unit but always in the ER (emergency department) or in the ER (emergency department) [20, 21].

3. SYSTEM METHODOLOGY

Compressing data increases transmission and reception efficiency. Compressed data can save database capacity and speed up data scans. This is evident in Telemedicine, which involves appropriate handling of enormous volumes of data from health sensors attached to isolated patients. Managing enormous volumes of data created by quick biomedical technologies is difficult. The technology intends to encrypt ECG signal files and transmit them in real time. Cryptography includes Encryption and Decryption. ECG signal encryption translates data into a decryption key or cipher text. Encryption algorithms and keys encrypt data or plaintext. Data encryption maintains the confidentiality of digital signal data. Due to varying monitoring needs, we created our own method to precisely and continually record heart rates. Most heart rate measuring procedures need physical contact.

3.1 Encrypting module

The fundamental procedure for ECG signal file encryption may be transmitted as a process of encryption in the module of encryptor, transmission to the decryptor module through a communication channel, original signal file retrieval at the output of the decryptor module [22, 23]. DFT and IDFT are the algorithms that are utilized. The encryption module offers the ability to encrypt a signal file, which renders it unreadable. The first step is to produce the signal file that has to be encrypted. This file's location is specified. The ECG data is broken down into individual characters, which are then transformed into ASCII codes [24, 25]. For further encryption, the codes are put via the DFT method. The outcome is a sequence of complex numbers. The needed encrypted output is produced after the DFT method has been run. The Figure 1, below refer to the system methodology of the proposed system. The encrypted output is stored and kept in the new file location seen in Figure 2 [26, 27].

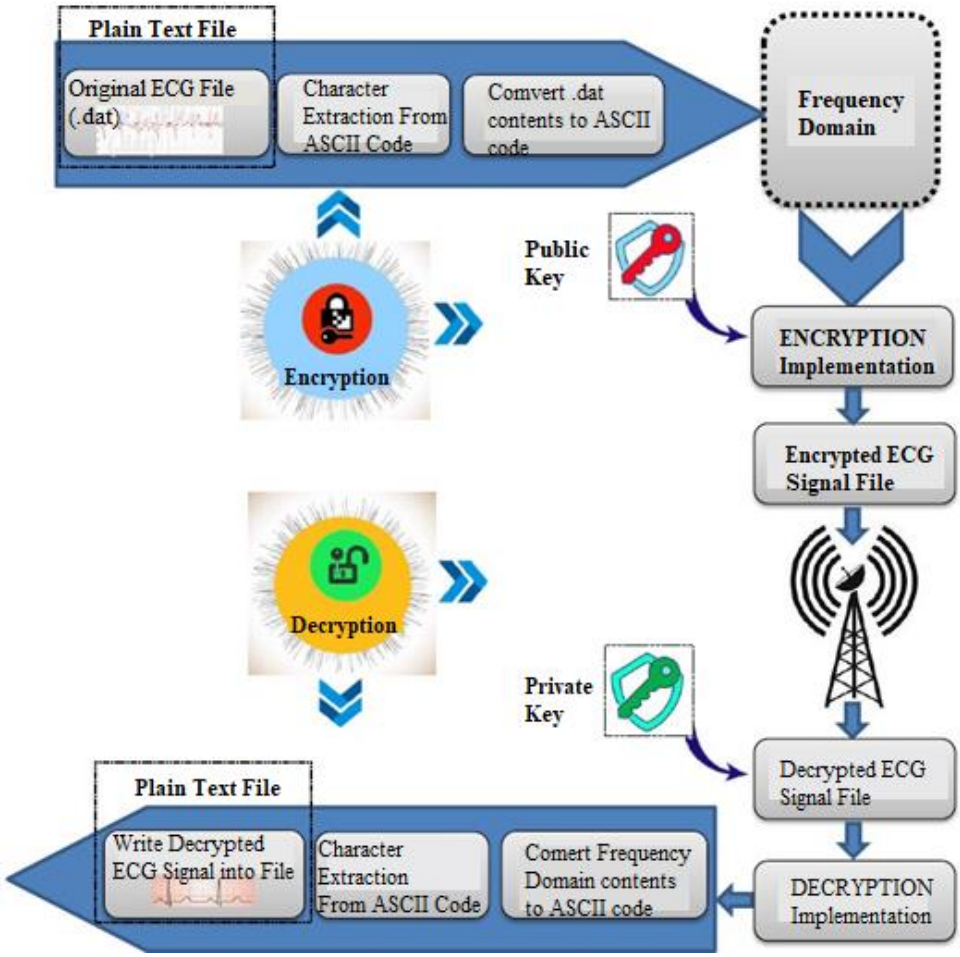

Figure 1. The proposed system methodology

Pseudo code for ECG data packets Encryption Algorithm
Step One. An alphanumeric array refers to (Set); and set length refer to (Len)**.**
Step Two. Square matrix [S]MXM equal to reshape [set]
Step Three. Divide the matrix [S] into 3- matrices of equal size named S1, S2, and S3
Step Four. Apply keys K1 for S1, K2 for S2, and K3 for S3 respectively to scale up
Step Five. Collect all 3- matrices into single matrix [C], where C – cipher_ text
Step Six. Array Re-arrange according to sync factor K4 equal to Y, where Y equal to {m,n}
Pseudo code for ECG data packets Decryption Algorithm
Step One: An array of not-a-number with 1 to N values refer to Length.
Step Two: Array Re-arrange according to K1& Convert it into square matrix [S]
Step Three: Split the [S] into 3- say d1, d2 and d3
Step Four: Apply the K2 for d1, K3 for d2, and K4 for d3.
Step Five: Collect the 3- parts into single matrix called [M]
Step Six: Utilizing the matrix [M], convert plain text.

3.2 Decrypting module

The decryptor module of the application, where the encrypted signal files are received from the encryptor, is another crucial component. The program's decryptor module provides the cryptographer with user-friendly and secure options [28, 29]. The user must first convert the encrypted data's path or file location in order to decrypt the data into readable form or recover it in its original form. The appropriate file must next be extracted in order for all coded characters extracted [30, 31]. The IDFT algorithm is then run on the file. This produces the necessary decrypted output data [32, 33]. The decryptor side's utilize of IDFT transforms frequency domain to time domain [34, 55].

4. BIOMEDICAL DATA ACQUIRING

From National Instruments, you can choose from a wide variety of data acquisition cards. Analog inputs and outputs are available on these cards. A DAQ card is also supported by LabVIEW with ready-made libraries. By utilizing these libraries, engineers can quickly and easily develop data acquisition programs, allowing them to spend more time processing and analyzing the acquired signals [5]. PCI-6023E from National Instruments was used. With its 16 analog input channels (eight differential) and two analog output channels, the 6025E features a 100-pin connector and 32 digital inputs and outputs. Featuring 68 pins, 8 digital I/O lines, 16 analog inputs, two analog outputs, and 16 analog inputs, the 6024E has 16 channels of analog inputs and outputs. There are no analog output channels on the 6023E, so it is similar to the 6024E [9, 18]. Every National Instruments DAQ system comes with the NI-DAQ driver software. The SCXI-1200 is the only accessory product that is packaged with NI-DAQ. Application programming environments can access NI-DAQ's extensive library of functions. Inputs (A/D conversion) buffered data acquisitions (high-speed A/D conversion), outputs (D/A conversion), waveform generation (timed D/A conversion), digital I/O, counters and timers, SCXI, self-

calibration, messaging, and data acquisition from extended memory are just a few of these functions. DAQ hardware and computers interact in many complicated ways, including interrupt programming and DMA controllers. You can change platforms without modifying your code since NIDAQ maintains a consistent software interface between versions. We use NI-DAQ driver software, regardless of whether we are using conventional programming languages or National Instruments software. Following the installation of NIDAQ device drivers on your computer, the MAX - Measurement and Automation Explorer icon will appear on the desktop. This program determines the presence of DAQ cards and the channel settings. A PCI-6023E DAQ acquisition card is accessible through Measurement and Automation Explorer (MAX). The MAX software from National Instruments allows users to manage devices, interfaces, installed software, virtual channels, and tasks. In addition to constructing scales for virtual instruments, configuring drivers, and importing and exporting configuration files, you can also create virtual instruments.

5. A COMPUTER-BASED METHOD FOR ANALYZING AND DISPLAYING BIOMEDICAL SIGNALS

In the human body, biomedical signals are typically very small, typically around millivolts, and each requires special processing. Microvoltage electroencephalography signals have many frequency components. In order to analyze these biomedical signals, they must first be processed. With LabVIEW, you can perform complex analysis with tools ranging from fast FTs to digital filters. Complex signals must be first broken down into their frequency components in order to perform frequency analysis. FFTs are commonly used for this. This type of analysis is made easy using LabVIEW's built-in FFTs, which allow fast and easy component separation. Noise overload is common with biomedical signals due to their small size. In order to overcome this problem, an SCXI card must be used, which involves filtering and amplification of the acquired signal. It is still possible for the signal to contain noise after it has reached the computer. You can also use LabVIEW's digital filters to solve the noise problem. Using LabVIEW, you can implement Butterworth, Bessel, Chebyshev, or digital filters. Almost any design can be adapted to these filters with a few adjustments. Express virtual instruments allow users to select different parameters from their internal implementation to perform a dual-channel spectral measurement with a filter. Biomedical signals are simulated using white noise DC signals. After the signal has been filtered in step one, it is filtered in step two using a bandpass filter. Second, we check to see if the upper and lower cut-off frequency models have changed since our last iteration, then update the Waveform Graph cursors with the new values. If this is the case, the second step will consist of measuring the spectral response of the filter on the prefiltered and filtered signals. Third, the prefiltered signal will be analyzed using Spectral Measurement; fourth, the cleaned signal will be analyzed using Spectral Measurement. A final test determines whether the filter meets the specifications by comparing the calculated frequency response with the preset specifications. The simulation used uniform white noise due to its wide frequency range. Due to its dual-channel capability, the Dual Channel Spectral Measurement Express virtual instrument can analyze.

6. RESULTS AND DISCUSSION

Based on Anti-attack Proposed Algorithm, there are three separate keys are utilized in the suggested attack, making Brute force attacks more difficult. The algorithm causes the most confusion, especially for collections of alphanumeric data. The strategy highly resists assaults that need knowledge of the key. Brute force attacks may be utilized against encryption relying on passwords. Table 1 lists the suggested technique in comparison to the literature. The result comprises encrypted and decrypted.dat files. First, create a LabVIEW VI. This VI has front and block diagrams. Figure 2 shows the front panel user interface. A block diagram of encryption has been completed. The location of the raw data (for the ECG signal).dat file was specified. The encrypted file's other path was given. The output of the encrypted binary is rebuilt in this file. The information from the original.dat file is turned into cipher text as a consequence of the encryption procedure, and it is replaced in the empty text file location that is given.

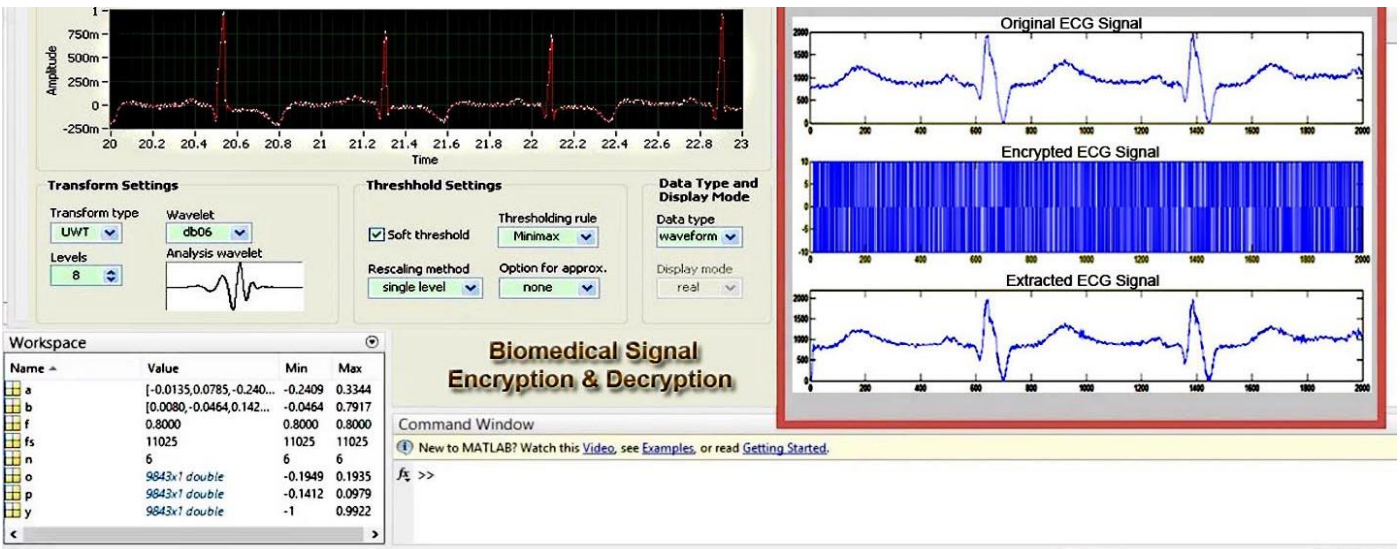

Figure 2. LabVIEW interface with three cases of ECG signal; Raw ECG signal, encrypted ECG signal, and decrypted ECG signals

Table 1. Lists the suggested technique in comparison to the literature

Attack Based on Literature	Brute Force	Cipher Text-Only	Chosen Cipher Text	The Size of Utilized Key
DES algorithm [6]	Agree	Nil	Nil	56 bits
Honey encrypt [3]	Agree	Nil	Nil	Related to message length
The proposed system	Disagree	Disagree	Disagree	Max. 3 keys each of size

7. CONCLUSION

There are only two threats to the confidentiality of medical information: while it is moving and when it is resting in storage facilities. The solution is achieved through the use of LabVIEW, which integrates several keys into a symmetric key algorithm. Data handling for alpha-numerics and numerics is separated. A database of patient's medical information may be maintained using this cryptographic method to keep less sensitive private information secure. Therefore, the proposed scheme provides adequate security for less sensitive private data with a lower computational burden.

ACKNOWLEDGMENT

A special thank you goes to the Iraqi Ministry of Higher Education and Scientific Research (MOHESR) for technical assistance.

REFERENCES

[1] Attiah, M.L., Md Isa, A.A., Zakaria, Z., Abdullah, N.F., Ismail, M., Nordin, R. (2018). Adaptive multi-state millimeter wave cell selection scheme for 5G communications. International Journal of Electrical & Computer Engineering, 8(5): 2967-2978. https://doi.org/10.11591/ijece.v8i5.pp2967-2978

[2] Liu, H., Kadir, A., Xu, C. (2020). Color image encryption with cipher feedback and coupling chaotic map. International Journal of Bifurcation and Chaos, 30(12): 2050173. https://doi.org/10.1142/S0218127420501734

[3] Noura, H., Guyeux, C., Chehab, A., Mansour, M., Couturier, R. (2019). Efficient chaotic encryption scheme with OFB mode. International Journal of Bifurcation and Chaos, 29(5): 1950059. https://doi.org/10.1142/S0218127419500597

[4] Abdulbaqi, A.S., Najim, S.A.D.M., Mahdi, R.H. (2018). Robust multichannel EEG signals compression model based on hybridization technique. International Journal of Engineering & Technology, 7(4): 3402-3405. https://doi.org/10.14419/ijet.v7i4.14513

[5] Singh, V.K., Singh, P.K., Rai, K.N. (2018). Image encryption algorithm based on circular shift in pixel bit value by group modulo operation for medical images. In 2018 4th International Conference on Computing Communication and Automation (ICCCA), Greater Noida, India, pp. 1-7. https://doi.org/10.1109/CCAA.2018.8777588

[6] Dey, N., Mukhopadhyay, S., Das, A., Chaudhuri, S.S. (2012). Analysis of P-QRS-T components modified by blind watermarking technique within the electrocardiogram signal for authentication in wireless telecardiology using DWT. International Journal of Image, Graphics and Signal Processing, 4(7): 33-46. https://doi.org/10.5815/ijigsp.2012.07.04.

[7] Ibaida, A., Khalil, I. (2013). Wavelet-based ECG steganography for protecting patient confidential information in point-of-care systems. IEEE Transactions on Biomedical Engineering, 60(12): 3322-3330. https://doi.org/10.1109/TBME.2013.2264539

[8] Chen, S.T., Guo, Y.J., Huang, H.N., Kung, W.M., Tseng, K.K., Tu, S.Y. (2014). Hiding patients confidential data in the ECG signal via transform-domain quantization scheme. Journal of Medical Systems, 38: 1-8. https://doi.org/10.1007/s10916-014-0054-9

[9] Fira, C.M., Goras, L. (2008). An ECG signals compression method and its validation using NNs. IEEE Transactions on Biomedical Engineering, 55(4): 1319-1326. https://doi.org/10.1109/TBME.2008.918465

[10] Lee, S., Kim, J., Lee, M. (2011). A real-time ECG data compression and transmission algorithm for an e-health device. IEEE Transactions on Biomedical Engineering, 58(9): 2448-2455. https://doi.org/10.1109/TBME.2011.2156794

[11] Mamaghanian, H., Khaled, N., Atienza, D., Vandergheynst, P. (2011). Compressed sensing for real-time energy-efficient ECG compression on wireless body sensor nodes. IEEE Transactions on Biomedical Engineering, 58(9): 2456-2466. https://doi.org/10.1109/TBME.2011.2156795

[12] Abo-Zahhad, M., Ahmed, S.M., Zakaria, A. (2012). An efficient technique for compressing ECG signals using QRS detection, estimation, and 2D DWT coefficients thresholding. Modelling and Simulation in Engineering, 2012: 742786. https://doi.org/10.1155/2012/742786

[13] Agulhari, C.M., Bonatti, I.S., Peres, P.L. (2013). An adaptive run length encoding method for the compression of electrocardiograms. Medical Engineering & Physics, 35(2): 145-153. https://doi.org/10.1016/j.medengphy.2010.03.003

[14] Ma, J., Zhang, T., Dong, M. (2014). A novel ECG data compression method using adaptive fourier decomposition with security guarantee in e-health applications. IEEE Journal of Biomedical and Health Informatics, 19(3): 986-994. https://doi.org/10.1109/JBHI.2014.2357841

[15] Adamo, A., Grossi, G., Lanzarotti, R., Lin, J. (2015). ECG compression retaining the best natural basis k-coefficients via sparse decomposition. Biomedical Signal Processing and Control, 15: 11-17. https://doi.org/10.1016/j.bspc.2014.09.002

[16] Jha, C.K., Kolekar, M.H. (2017). ECG data compression algorithm for tele-monitoring of cardiac patients. International Journal of Telemedicine and Clinical Practices, 2(1): 31-41. https://doi.org/10.1504/IJTMCP.2017.082106

[17] Elgendi, M., Mohamed, A., Ward, R. (2017). Efficient ECG compression and QRS detection for e-health applications. Scientific Reports, 7(1): 459. https://doi.org/10.1038/s41598-017-00540-x

[18] Elgendi, M., Al-Ali, A., Mohamed, A., Ward, R. (2018). Improving remote health monitoring: A low-complexity ECG compression approach. Diagnostics, 8(1): 10.

https://doi.org/10.3390/diagnostics8010010
[19] Sinha, S., Makkar, P. (2021). Wireless sensor networks: Concepts, components, and challenges. In Security and Privacy Issues in IoT Devices and Sensor Networks, pp. 1-27. Academic Press. https://doi.org/10.1016/B978-0-12-821255-4.00001-8
[20] Wanda, P., Jie, H.J. (2018). Efficient data security for mobile instant messenger. TELKOMNIKA (Telecommunication Computing Electronics and Control), 16(3): 1426-1434. https://doi.org/10.12928/telkomnika.v16i4.4045
[21] Mahmood, S.D., Hutaihit, M.A., Abdulrazaq, T.A., Abdulbaqi, A.S., Tawfeeq, N.N. (2021). A telemedicine based on EEG signal compression and transmission. Technology, 18(SI05): 894-913. https://doi.org/10.14704/web/v18si05/web18270
[22] Liu, Y., Qin, Z., Liao, X., Wu, J. (2020). Cryptanalysis and enhancement of an image encryption scheme based on a 1-D coupled Sine map. Nonlinear Dynamics, 100: 2917-2931. https://doi.org/10.1007/s11071-020-05654-y
[23] Boussif, M., Aloui, N., Cherif, A. (2018). Secured cloud computing for medical data based on watermarking and encryption. IET Networks, 7(5): 294-298. https://doi.org/10.1049/iet-net.2017.0180
[24] Parameshachari, B.D., Panduranga, H.T., liberata Ullo, S. (2020). Analysis and computation of encryption technique to enhance security of medical images. IOP Conference Series: Materials Science and Engineering, 925(1): 012028. https://doi.org/10.1088/1757-899x/925/1/012028
[25] Naveen, M., Babu, G.S. (2018). An extensive survey on image security research trends. Communications on Applied Electronics, 7(13): 21-26. https://doi.org/10.5120/cae2018652751
[26] Nirenjena, S., Jayapriya, M. (2020). A novel triple layer method to hide secret image using steganography. In 2020 International Conference on System, Computation, Automation and Networking (ICSCAN), Pondicherry, India, pp. 1-7. https://doi.org/10.1109/ICSCAN49426.2020.9262406
[27] Putra, S.D., Ahmad, A.S., Sutikno, S., Kurniawan, Y., Sumari, A.D.W. (2018). Revealing AES encryption device key on 328P microcontrollers with differential power analysis. International Journal of Electrical and Computer Engineering, 8(6): 5144-5152. https://doi.org/10.11591/ijece.v8i6.pp.5144-5152
[28] Tripathy, A.K., Das, T.K., Navaneethan, C. (2019). Data cryptography based on musical notes on a fingerboard along with a dice. Indonesian Journal of Electrical Engineering and Computer Science, 14(3): 1286-1290. https://doi.org/10.11591/ijeecs.v14.i3.pp1286-1290
[29] Peyghami, S., Blaabjerg, F. (2020). Availability modeling in power converters considering components aging. IEEE Transactions on Energy Conversion, 35(4): 1981-1984. https://doi.org/10.1109/TEC.2020.3018631
[30] Qayyum, A., Ahmad, J., Boulila, W., Rubaiee, S., Masood, F., Khan, F., Buchanan, W.J. (2020). Chaos-based confusion and diffusion of image pixels using dynamic substitution. IEEE Access, 8: 140876-140895. https://doi.org/10.1109/ACCESS.2020.3012912
[31] Shah, S. A., Ahmad, J., Masood, F., Shah, S.Y., Pervaiz, H., Taylor, W., Imran, M.A., Abbasi, Q.H. (2020). Privacy-preserving wandering behavior sensing in dementia patients using modified logistic and dynamic newton leipnik maps. IEEE Sensors Journal, 21(3): 3669-3679. https://doi.org/10.1109/JSEN.2020.3022564
[32] Abdulbaqi, A.S. (2019). Recruitment internet of things for medical condition assessment: Electrocardiogram signal surveillance. AUS Journal, Institute of Architecture and Urbanism, University of Austral de Chile, Special, (2019): 434-440.
[33] Roslin, S.E., Nandhitha, N.M., Daniel, A. (2014). Transposition based symmetric encryption and decryption technique for secured image transmission through internet. In 2014 International Conference on Circuits, Power and Computing Technologies [ICCPCT-2014], Nagercoil, India, pp. 1578-1583. https://doi.org/10.1109/ICCPCT.2014.7055035
[34] Alawida, M., Teh, J.S., Samsudin, A. (2019). An image encryption scheme based on hybridizing digital chaos and finite state machine. Signal Processing, 164: 249-266. https://doi.org/10.1016/j.sigpro.2019.06.013
[35] Faisal, G.M., Alshadoodee, H.A.A., Abbas, H.H., Gheni, H.M., Al-Barazanchi, I. (2022). Integrating security and privacy in mmWave communications. Bulletin of Electrical Engineering and Informatics, 11(5): 2856-2865. https://doi.org/10.11591/eei.v11i5.4314
[36] Al-Barazanchi, I., Hashim, W., Alkahtani, A.A., Abdulshaheed, H.R., Gheni, H.M., Murthy, A., Daghighi, E., Shawkat, S.A., Jaaz, Z.A. (2022). Remote monitoring of COVID-19 patients using multisensor body area network innovative system. Computational Intelligence and Neuroscience, 2022: 9879259. https://doi.org/10.1155/2022/9879259
[37] Niu, Y., Kadhem, S.I., Al Sayed, I.A., Jaaz, Z.A., Gheni, H.M., Al Barazanchi, I. (2022). Energy-saving analysis of wireless body area network based on structural analysis. In 2022 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA), Ankara, Turkey, pp. 1-6. https://doi.org/10.1109/HORA55278.2022.9799972
[38] Al Barazanchi, I., Abdulshaheed, H.R., Jaaz, Z.A., Gheni, H.M., Niu, Y., Almutairi, H., Daghighi, E., Shawkat, S.A., Ahmed, S.R. (2022). Blockchain: The next direction of digital payment in drug purchase. In 2022 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA), Ankara, Turkey, pp. 1-7. https://doi.org/10.1109/HORA55278.2022.9799993
[39] Al-Barazanchi, I., Abdulshaheed, H.R., Sidek, M.S.B. (2019). A survey: Issues and challenges of communication technologies in WBAN. Sustainable Engineering and Innovation, 1(2): 84-97. http://doi.org/10.37868/sei.v1i2.85
[40] Shawkat, S.A., Al-Barazanchi, I. (2022). A proposed model for text and image encryption using different techniques. TELKOMNIKA (Telecommunication Computing Electronics and Control), 20(4): 858-866. http://doi.org/10.12928/telkomnika.v20i4.23367
[41] Al_Barazanchi, I., Niu, Y., Abdulshaheed, H.R., Hashim, W., Alkahtani, A.A., Daghighi, E., Jaaz, Z.A., Shawkat, S.A., Rauf, H.T. (2022). Proposed a new framework scheme for the path loss in wireless body area network. Iraqi Journal for Computer Science and Mathematics, 3(1): 11-21. https://doi.org/10.52866/ijcsm.2022.01.01.002
[42] Abdulshaheed, H.R., Abbas, H.H., Ahmed, E.Q., Al-Barazanchi, I. (2022). Big data analytics for large scale

wireless body area networks; Challenges, and applications. In: Saeed, F., Mohammed, F., Ghaleb, F. (eds) Advances on Intelligent Informatics and Computing. IRICT 2021. Lecture Notes on Data Engineering and Communications Technologies, vol 127. Springer, Cham. https://doi.org/10.1007/978-3-030-98741-1_35

[43] Oleiwi, S.S., Mohammed, G.N., Al_barazanchi, I. (2022). Mitigation of packet loss with end-to-end delay in wireless body area network applications. International Journal of Electrical and Computer Engineering, 12(1): 460-470. https://doi.org/10.11591/ijece.v12i1.pp460-470

[44] Ali, A.M., Ngadi, M.A., Al_Barazanchi, I.I., JosephNg, P.S. (2023). Intelligent traffic model for unmanned ground vehicles based on DSDV-AODV protocol. Sensors, 23(14): 6426. https://doi.org/10.3390/s23146426

[45] Salih, S.Q., Alsewari, A.A., Yaseen, Z.M. (2019). Pressure vessel design simulation: Implementing of multi-swarm particle swarm optimization. In Proceedings of the 2019 8th International Conference on Software and Computer Applications, pp. 120-124. https://doi.org/10.1145/3316615.3316643

[46] Salih, S.Q. (2019). A new training method based on black hole algorithm for convolutional neural network. Journal of Southwest Jiaotong University, 54(3): 1-10. https://doi.org/10.35741/issn.0258-2724.54.3.22

[47] Malik, A., Rai, P., Heddam, S., Kisi, O., Sharafati, A., Salih, S.Q., Al-Ansari, N., Yaseen, Z. M. (2020). Pan evaporation estimation in Uttarakhand and Uttar Pradesh States, India: Validity of an integrative data intelligence model. Atmosphere, 11(6): 553. https://doi.org/10.3390/atmos11060553

[48] Tao, H., Awadh, S.M., Salih, S.Q., Shafik, S.S., Yaseen, Z.M. (2022). Integration of extreme gradient boosting feature selection approach with machine learning models: application of weather relative humidity prediction. Neural Computing and Applications, 34(1): 515-533. https://doi.org/10.1007/s00521-021-06362-3

[49] Malik, A., Kumar, A., Kisi, O., Khan, N., Salih, S.Q., Yaseen, Z.M. (2021). Analysis of dry and wet climate characteristics at Uttarakhand (India) using effective drought index. Natural Hazards, 105: 1643-1662. https://doi.org/10.1007/s11069-020-04370-5

[50] Tao, H., Al-Sulttani, A.O., Salih Ameen, A.M., Ali, Z.H., Al-Ansari, N., Salih, S.Q., Mostafa, R.R. (2020). Training and testing data division influence on hybrid machine learning model process: Application of river flow forecasting. Complexity, 2020: 1-22. https://doi.org/10.1155/2020/8844367

[51] Karimi, B., Mohammadi, P., Sanikhani, H., Salih, S.Q., Yaseen, Z.M. (2020). Modeling wetted areas of moisture bulb for drip irrigation systems: An enhanced empirical model and artificial neural network. Computers and Electronics in Agriculture, 178: 105767. https://doi.org/10.1016/j.compag.2020.105767

[52] Cui, F., Salih, S.Q., Choubin, B., Bhagat, S.K., Samui, P., Yaseen, Z.M. (2020). Newly explored machine learning model for river flow time series forecasting at Mary River, Australia. Environmental Monitoring and Assessment, 192: 1-15. https://doi.org/10.1007/s10661-020-08724-1

[53] Hai, T., Bhuiyan, M.Z.A., Wang, J., Wang, T., Hsu, D.F., Li, Y., Salih, S.Q., Wu, J., Liu, P. (2020). DependData: Data collection dependability through three-layer decision-making in BSNs for healthcare monitoring. Information Fusion, 62: 32-46. https://doi.org/10.1016/j.inffus.2020.03.004

[54] Salih, S.Q., Habib, M., Aljarah, I., Faris, H., Yaseen, Z.M. (2020). An evolutionary optimized artificial intelligence model for modeling scouring depth of submerged weir. Engineering Applications of Artificial Intelligence, 96: 104012. https://doi.org/10.1016/j.engappai.2020.104012

[55] Al-Juboori, S.A.M., Hazzaa, F., Jabbar, Z.S., Salih, S., Gheni, H.M. (2023). Man-in-the-middle and denial of service attacks detection using machine learning algorithms. Bulletin of Electrical Engineering and Informatics, 12(1): 418-426. https://doi.org/10.11591/eei.v12i1.4555