CORRECTED VERSION: Integrating a Secure and Low-Cost WSN Layer with Medical Cloud Computing for Medical Image Transmission

Israa Hussain Abd Alla[1], Falath M.Mohammed[2], Saif Al-din M. N[3], Azmi Shawkat Abdulbaqi[4,*]

[1]Ministry of Education, Open Educational College, Baghdad, Al-Karkh-3, Iraq

[2]College of Education for Humanities, Geography Department, Ramadi, Iraq

[3]University of Anbar, College of Computer and Information Technology, Ramadi, Iraq

[4]University of Anbar, Renewable Energy Research Center, Ramadi, Iraq

Emails: Israa_hussain@yahoo.com; falath1972@uoanbar.edu.iq; saifaddin.r@uoanbar.edu.iq; azmi_msc@uoanbar.edu.iq

Abstract

Throughout a Wireless Sensor Network (WSN), information collected from the environment is continuously transmitted from one node to the next, and then the main collector or server receives and processes it. With the growth of a network, data transfers within the network also grow dramatically. Medical images increase traffic on a network if they are transmitted. An interlayer transmission protocol (WSN) was developed for this study. Pixels are used to create the medical image using the protocol. A gray-level medical image with 512x512 pixels provided by Brain was used to conduct the study. Medical image size is reduced from 256 KB to 192 KB, providing a 25% advantage. A study found SSIM of 51, 1365 and PSNR of 0,9976 for the structural similarity ratio (SSIM). The Advanced Encryption Standard (AES) encryption algorithm safeguards data during the transfer. By creating such a layer, transmissions became safer. In the WSNs, 12.5% and 25% of the data transfer has been reduced based on the information obtained from the study without changing the medical image.

Keywords: WSNs (Wireless Sensors Networks); Medical Image Transmission; Structural Similarity Ratio (SSIM)

1. Introduction

The WSNs are used for security, disaster response, and surveillance of wars, manufacturing automation, healthcare, and environmental preservation, among many other things. Secure and reliable data transmission is required for all of the applications listed above [1][2]. There is usually a limited amount of power, memory, and bandwidth available for WSNs since they are generally ad-hoc networks. In the Internet environment, WSN systems can integrate a large number of sensor devices because of new technological developments. Military, industrial, health, and emergency management applications have been developed for WSNs. Data-based applications can be developed on either text or image bases [3][4]. If medical image transfers are performed in these networks, where hardware is already limited, optimize the data being transferred. The WSN can transmit medical image, videos, and secret data. It is vital that sensor nodes have a high level of quality and security in this process [5][6]. An attempt was made to transfer medical images in wireless networks more effectively and efficiently. The data traffic caused by sending more images has been reduced and secured by creating a new transmission layer. It uses pixels from the medical image to create the transmission layer. Medical images are formed by the "least important bits" (LSB) of each pixel. Channel security and encrypting the transported data were achieved using the AES algorithm [7][8]. As a result, the article was arranged as follows; Section2 includes the Methodology of the System. Section 3, presented System Implementation. The Transmission / Receiving Side introduced in Section 3.

DOI: https://doi.org/10.54216/FPA.180103
Received: June 18, 2024 Revised: September 17, 2024 Accepted: December 22, 2024 Corrected: December 11, 2025

2. System Methodology

Two-dimensional vector arrays are used in digital medical images. A matrix with a vector as each element is another way of expressing it. Medical images consist of two independent variables that form x and y geometric dimensions. Pixels refer to the area of a medical image in which f (x, y) shows any value. Digital medical images consist of pixels, which are the smallest unit of information. Various methods are used to process medical images digitally. The coordinate system described above can be used to classify binary, grayscale, and color images.

A. Medical Image with Gray Level

An image's pixel values can determine the type of medical image. Black and white are the two colors that appear on the borders of gray-level images. A gray-scale (monochromatic) image is encoded between these two[9][10]. There are eight bits encoded for each pixel in the application. An image of this type consists of 256 discrete gray tones (brightness levels), the format of which is as follows G=[0, 1, 2,...,255}. Generally, black is represented by 0 gray levels, white by a 255 gray level, and gray tones by gray levels between these values. The gray level grid incorporates 256 different gray levels [11][12].

B. Bit with the least significance (LSB)

A common steganographic technique is LSB Insertion. LSB stands for the in a pixel's bits. When 00100111 is the value of the pixel, it represents the LSB in that pixel by the rightmost value of 1, which is bolded. The human eye is unable to detect a change when this bit is changed in a pixel[13][14]. A pixel with a value of 01101101 that is given a color code of 109 will have a new pixel value equal to 01101100, which indicates that it is assigned a value of 108 when the last bit is changed. Human eyes cannot distinguish between the 108 and 109 color codes because the differences between them are too small [15][16].

C. Noise Ratio of Peak Signals (PSNR)

An objective measure of medical image quality is the PSNR [17]. PSNRs of original and distorted medical images are compared after the original medical images are controlled and degraded. For images of 8 bits, PSNR is calculated according to equation 2[18][19]. Based on equation 2, the C parameter shows the original medical image and ST shows the noisy medical image. When the PSNR value is higher, an image has a better quality. If two images have different PSNR values, the difference is great [20][21].

D. Structural Similarity Measure (SSIM)

Three characteristics of the images are compared in this method: brightness, contrast, and structure. Equation 2 below identifies the SSIM criterion, the x, and the y images [22][23].

$$SSIM(x,y) = \frac{(2\mu_x\mu_y+C_1)(2\sigma_{xy}+C_2)}{(\mu_x^2+\mu_y^2+C_1)(\mu_x^2+\mu_y^2+C_2)} \quad (2)$$

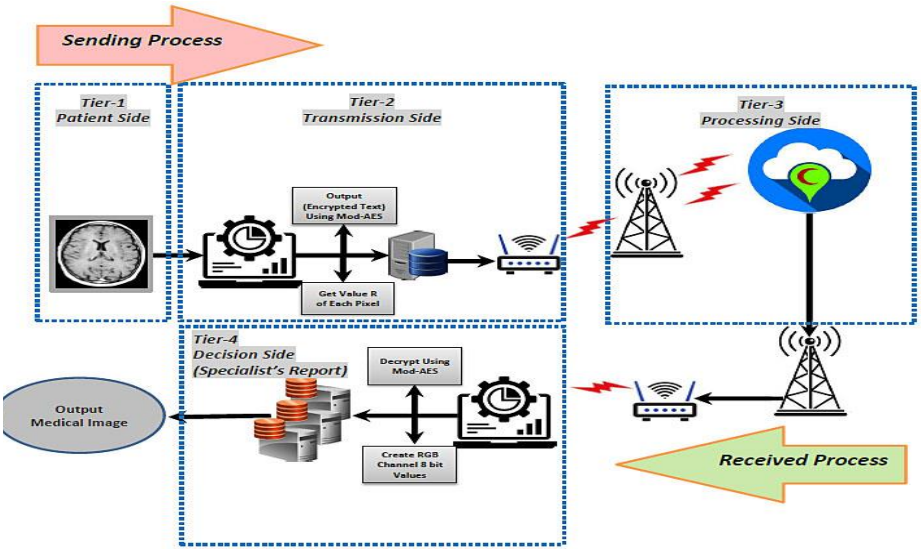

Figure 1. The Infrastructure of the Proposed System

DOI: https://doi.org/10.54216/FPA.180103
Received: June 18, 2024 Revised: September 17, 2024 Accepted: December 22, 2024 Corrected: December 11, 2025

In this case, the estimated image is illustrated by comparing the images $\mu_x, \mu_{y,\sigma_x,\sigma_y}$, and $\sigma_{xy}$and determining the average pixel density, the standard deviation, and the common variance[24] [25]. A developed transmission layer utilizes the tiniest bits of each pixel for the image. To begin with, we discarded the last pixel, then we discarded the last two pixels.. Brain image (Figure 4) was analyzed using a 512×512 pixel image [26][27].

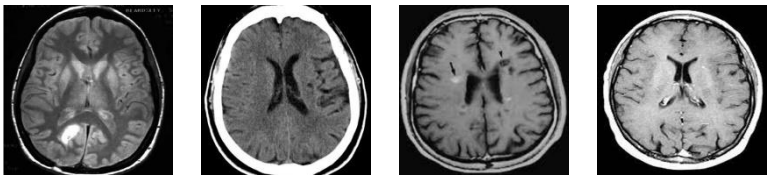

Figure 2. Different Brain Images with Size 512×512

E. Modified AES (Mod-AES) Algorithm

There is a modification in the AES algorithm where an additional key generation step occurs around the key generation step [28][29]. The original step of the algorithm is similar, but the modification takes place as shown in the next section; where: (1) Create another key (key2) a. Seeding b. Based on the seed, an 8-bit LFSR produces a matrix of 256 keys c[30]. Randomly select a number from the LFSR matrix for each round to indicate the key (Key 2) (2)In step 2, key1, key2, and the original text are XOR'd (3) Reduce the number of rounds to half the original number[31][32].

3. System Implementation

One last pixel remains in a medical image if this method is used. Thus, the compressed image ended up with 227 KB rather than 256 KB. Consequently, 12.5% was saved on overall costs. Text strings are constructed by adding together these seven bits and discarding the remaining bits[32][33]. Each pixel is copied only in its last bit; its other 7 bits are not copied. Consequently, the recipient received a text string. A reconstruction requires adding back in previously discarded bits [34]. Because their locations are not hidden, dropped pixels are randomly added to the image. Image changes are not significant when random bits are inserted. In figure 2, the original image's pixels were given last-bit values to create a new image [16].

Figure 3. Randomly Last Bits generated in The Medical Image

Both images are almost identical according to PSNR and SSIM values derived from comparisons of the original and subsequent images. In Table 1, PSNR and SSIM values are presented. Before transferring data, encrypting the text string will increase its security [22][23]. An unauthorized person can access all the data if the transmission line does not have a password. Encryption was performed using the Mod-AES algorithm. Mod-AES does not distinguish between clear text and plain text in terms of data size. The data is not increased during encryption. Both sender/receiver utilize the same algorithms to implement the scheme in Figure 3[24][25].

The infrastructure of the *Sender* Part (Transmission Side) and *Receiver* Part (Receiving Side) can be described as the following Figure 4, A and B:

4. Results and Discussion

By reducing the image size by 25%, the amount of data that must be transferred has been reduced. A single image seems to have a very small data size, but a network that continually shares images has a high data rate. For a wireless sensor network powered by 100 nodes sending 10 images per minute, the data required per minute would be 256 MB, the hourly data 15GB, and the daily data 360GB. Data of 360 GB per day has been reduced to 270 GB with a reduction of 25%, making it a perfect solution for reduced data by 25%. The limitations of these networks, as well as the fact that they transfer less data, will also extend the battery life of their devices. Images

DOI: https://doi.org/10.54216/FPA.180103
Received: June 18, 2024 Revised: September 17, 2024 Accepted: December 22, 2024 Corrected: December 11, 2025

created after the transfer may contain visible or even invisible differences. When it comes to transferring identical images, this method fails. Loss transfers are performed using this method. The PSNR and SSIM values for a new medical image can be found in Table 1[26][27].

Table 1: A new medical image's PSNR and SSIM values

	PSNRs	SSIMs	Decrease Ration	The Size of the File
Med_Image 1	50.1265	0.8976	14.5 %	227 KB
Med_Image 2	43.2056	0.8879	26 %	189 KB
Med_Image 3	52.4322	0.7896	12.51 %	241 KB
Med_Image 4	46.6481	0.6598	10.4 %	188 KB
Med_Image 5	49.6402	0.6197	19 %	200 KB

Gray-level images were used in the study. Brain images in grayscale were taken with 512 x 512 pixels. When the last bit in each pixel was discarded, the image, which had originally been 256 KB, was reduced to 227 KB, 189 KB, 241 KB, 188 KB, and 200 KB, respectively. This method of transmitting images offers advantages of 14.5%, 26.5%, 12.51 %, 19 %, and 10.4%. When the last bit is randomly added to the receiver, the recreated image is compared with the original image. Based on a comparison of five images, the PSNR value for one bit discarded image was 44.2156 and the SSIM value for the other bit-discarded image was 48.2565, 43.2056, 52.4322, 46.6481, and 49.6402, while the PSNR values for the other bit-discarded image were 50.1265, 43.2056, 52.4322, 46.6481, and 49.6402. Study results found that high PSNR values indicate a low numerical difference between the original and newly created images, while low PSNR values indicate a high degree of similarity. Based on the SSIM values, the five images appear to be very similar. Through a transfer, layer that offers data gains without changing the image, this study obtained 12.5% and 25% data gains and reduced data traffic in wireless sensor networks. As a result, the sensor nodes consume less energy and last longer since the transfer process has been reduced [23][24]. Compression ratios will be increased in the next study depending on character count and frequency of occurrence. We compare the correlation coefficients between adjacent pixels in Table 2 using the original medical images and encrypted medical images [25-37].

Table 2: Calculate the correlation coefficient between adjacent pixels using both the original and encrypted medical images.

The Size of The Medical Image	Image_Direction	Plain Image	Cipher Image
Chest_Img 128*128	A Horizontal_View	0.8034	-0.09212
	The Vertical_View	0.8403	-0.1011
	The Diagonal_View	0.7953	-0.1016
Brain_Img 256*256 (White Background)	A Horizontal_View	0.8667	-0.10394
	The Vertical_View	0.8458	-0.10388
	The Diagonal_View	0.8821	-0.10474
Brain_Img 512*512 (Black Background)	A Horizontal_View	0.8775	-0.13986
	The Vertical_View	0.8845	-0.12198
	The Diagonal_View	0.8634	-0.1672

An analysis of the quality of medical images showed in Table 3.

DOI: https://doi.org/10.54216/FPA.180103
Received: June 18, 2024 Revised: September 17, 2024 Accepted: December 22, 2024 Corrected: December 11, 2025

Table 3: Image Quality Measures in Three Medical Imaging

Image Size	Parameter	Mod-AES	MAES
Chest.jpg (128×128)	MSE	0.1067	0.1065
	PSNR	59.147	59.1501
Brain.jpg (256×256) (Black Background)	MSE	0.119	0.1189
	PSNR	59.9671	59.9714
Brain.jpg (512×512) (Black Background)	MSE	0.1183	0.1182
	PSNR	59.4578	59.4581

5. Conclusion

When compared to normal image transmission, this data transmission layer saves 25% compared to lossy image transfer. Even though the image looks very similar to the original, it may not be appropriate for applications that require the image to be transferred. In contrast, other applications will benefit from the saved data.

References

[1]. Zhao, G., Yang, X., Zhou, B., and Wei, W., "RSA-based digital image encryption algorithm in wireless sensor networks," in Proc. 2010 2nd Int. Conf. Signal Processing Systems, vol. 2, pp. V2-640–643, Jul. 2010.

[2]. Bisht, N., Thomas, J., and Thanikaiselvan, V., "Implementation of security algorithm for wireless sensor networks over multimedia images," in Proc. 2016 Int. Conf. Communication and Electronics Systems (ICCES), pp. 1–6, Oct. 2016.

[3]. Mahrous, A. M., Moustafa, Y. M., and El-Ela, M. A. A., "Physical characteristics and perceived security in urban parks: Investigation in the Egyptian context," Ain Shams Engineering Journal, vol. 9, no. 4, pp. 3055–3066, Dec. 2018.

[4]. Aminudin, N., Maseleno, A., Shankar, K., Hemalatha, S., Sathesh Kumar, K., Fauzi1, et al., "Nur algorithm on data encryption and decryption," Int. J. Engineering & Technology, vol. 7, no. 2.26, pp. 109–118, 2018.

[5]. Ilayaraja, M., Shankar, K., and Devika, G., "A modified symmetric key cryptography method for secure data transmission," Int. J. Pure and Applied Mathematics, vol. 116, no. 10, pp. 301–308, 2017.

[6]. Shankar, K., and Eswaran, P., "An efficient image encryption technique based on optimized key generation in ECC using genetic algorithm," in Advances in Intelligent Systems and Computing, vol. 394, pp. 705–714, New York: Springer, 2016.

[7]. JayaLakshmi, G., Khalaf, H. A., Farhadi, A., Al Barzinji, S. M., Mahmood, S. D., Najim, S. A. D. M., et al., "Detection of COVID-19 from radiology modalities and identification of prognosis patterns," Int. J. Nonlinear Analysis and Applications, vol. 13, no. 1, pp. 1351–1365, 2022.

[8]. Darwish, A., Hassanien, A. E., Elhoseny, M., Sangaiah, A. K., and Muhammad, K., "The impact of the hybrid platform of internet of things and cloud computing on healthcare systems: opportunities, challenges, and open problems," J. Ambient Intelligence and Humanized Computing, pp. 1–16, 2017. DOI: 10.1007/s12652-017-0659-1.

[9]. Lee, S., Jeong, S., Chung, Y., Cho, H., and Pan, S. B., "Secure and energy-efficient image transmission for wireless sensor networks," in Proc. 2011 IEEE Ninth Int. Symp. Parallel and Distributed Processing with Applications Workshops, pp. 137–140, May 2011.

[10]. Rekha, R. N., and PrasadBabu, M. S., "On some security issues in pervasive computing- lightweight cryptography," Int. J. Computer Science and Engineering, vol. 4, no. 2, pp. 267, 2012.

[11]. Sathesh Kumar, K., Shanka, K., Ilayaraja, M., and Rajesh, M., "Sensitive data security in cloud computing aid of different encryption techniques," J. Advanced Research in Dynamical and Control Systems, vol. 9, pp. 2888–2899, 2018.

[12]. Gupta, D., Khanna, A., Shankar, K., Furtado, V., and Rodrigues, J. J., "Efficient artificial fish swarm based clustering approach on mobility aware energy-efficient for MANET," Trans. Emerging Telecommunications Technologies, pp. 1–10, 2018. DOI: 10.1002/ett.3524.

[13]. Bokhari, M. U., and Hassan, S., "A comparative study on lightweight cryptography," in Cyber Security: Proceedings of CSI 2015, pp. 69–79, Singapore: Springer, 2018.

[14]. Mary, I. R. P., Eswaran, P., and Shankar, K., "Multi secret image sharing scheme based on DNA cryptography with XOR," Int. J. Pure and Applied Mathematics, vol. 118, no. 7, pp. 393–398, 2018.

DOI: https://doi.org/10.54216/FPA.180103
Received: June 18, 2024 Revised: September 17, 2024 Accepted: December 22, 2024 Corrected: December 11, 2025

[15]. Manifavas, C., Hatzivasilis, G., Fysarakis, K., and Rantos, K., "Lightweight cryptography for embedded systems—A comparative analysis," in Data Privacy Management and Autonomous Spontaneous Security, pp. 333–349, Berlin, Heidelberg: Springer, 2013.
[16]. Sehrawat, D., and Gill, N. S., "Lightweight block ciphers for IoT based applications: A review," J. Applied Engineering Research, vol. 13, no. 5, pp. 2258–2270, 2018.
[17]. Elhoseny, M., Yuan, X., El-Minir, H. K., and Riad, A. M., "An energy efficient encryption method for secure dynamic WSN," Security and Communication Networks, vol. 9, no. 13, pp. 2024–2031, 2016.
[18]. Elhoseny, M., Elminir, H., Riad, A., and Yuan, X., "A secure data routing schema for WSN using elliptic curve cryptography and homomorphic encryption," J. King Saud University—Computer and Information Sciences, vol. 28, no. 3, pp. 262–275, 2016.
[19]. Wang, X. Y., and Gu, S. X., "New chaotic encryption algorithm based on chaotic sequence and plain text," IET Information Security, vol. 8, no. 3, pp. 213–216, 2014.
[20]. Shankar, K., and Lakshmanaprabu, S. K., "Optimal key based homomorphic encryption for color image security aid of ant lion optimization algorithm," Int. J. Engineering & Technology, vol. 7, no. 1.9, pp. 22–27, 2018.
[21]. Shehab, A., Elhoseny, M., Muhammad, K., Sangaiah, A. K., Yang, P., Huang, H., et al., "Secure and robust fragile watermarking scheme for medical images," IEEE Access, vol. 6, pp. 10269–10278, 2018. DOI: 10.1109/access.2018.2799240.
[22]. Ping, N. L., Ee, K. B., and Wei, G. C., "A study of digital watermarking on medical image," in World Congress on Medical Physics and Biomedical Engineering 2006, pp. 2264–2267, Berlin, Heidelberg: Springer, 2007.
[23]. Elhoseny, M., Shankar, K., Lakshmanaprabu, S. K., Maseleno, A., and Arunkumar, N., "Hybrid optimization with cryptography encryption for medical image security in internet of things," in Neural Computing and Applications, pp. 1–15, 2018.
[24]. Shankar, K., Elhoseny, M., Kumar, R. S., Lakshmanaprabu, S. K., and Yuan, X., "Secret image sharing scheme with encrypted shadow images using optimal homomorphic encryption technique," J. Ambient Intelligence and Humanized Computing, pp. 1–13, 2018.
[25]. Hatzivasilis, G., Fysarakis, K., Papaefstathiou, I., and Manifavas, C., "A review of lightweight block ciphers," J. Cryptographic Engineering, vol. 8, no. 2, pp. 141–184, 2018.
[26]. Hong, D., Sung, J., Hong, S., Lim, J., Lee, S., Koo, B. S., et al., "HIGHT: A new block cipher suitable for low-resource device," in Proc. Int. Workshop Cryptographic Hardware and Embedded Systems, pp. 46–59, Berlin, Heidelberg: Springer, Oct. 2006.
[27]. Bin Shibghatullah, A. S., "Mitigating developed persistent threats (APTs) through machine learning-based intrusion detection systems: A comprehensive analysis," SHIFRA, vol. 1, pp. 1–10, 2023. DOI: 10.70470/SHIFRA/2023/003.
[28]. Al Barazanchi, I. I., and Hashim, W., "Enhancing IoT device security through blockchain technology: A decentralized approach," SHIFRA, vol. 1, pp. 1–8, 2023. DOI: 10.70470/SHIFRA/2023/002.
[29]. Burhanuddin, M., "Assessing the vulnerability of quantum cryptography systems to emerging cyber threats," SHIFRA, vol. 1, pp. 1–8, 2023. DOI: 10.70470/SHIFRA/2023/004.
[30]. Aljohani, A., "Zero-trust architecture: Implementing and evaluating security measures in modern enterprise networks," SHIFRA, vol. 1, pp. 1–13, 2023. DOI: 10.70470/SHIFRA/2023/008.
[31]. Hashim, W., and Hussein, N. A.-H. K., "Securing cloud computing environments: An analysis of multi-tenancy vulnerabilities and countermeasures," SHIFRA, vol. 9, pp. 9–17, 2024. DOI: 10.70470/SHIFRA/2024/002.
[32]. Sarsam, S. M., "Cybersecurity challenges in autonomous vehicles: Threats, vulnerabilities, and mitigation strategies," SHIFRA, vol. 1, pp. 1–9, 2023. DOI: 10.70470/SHIFRA/2023/005.
[33]. Gupta, S., Kumar, S., and Mishra, A., "Human-centric approach for cybersecurity: Understanding the impact of human behavior on security incidents and mitigation strategies," *Computers & Security*, vol. 104, pp. 102146, 2021. DOI: 10.1016/j.cose.2021.102146.
[34]. Tambe-Jagtap, S. N., "A survey of cryptographic algorithms in cybersecurity: From classical methods to quantum-resistant solutions," SHIFRA, vol. 1, pp. 1–10, 2023. DOI: 10.70470/SHIFRA/2023/006.

DOI: https://doi.org/10.54216/FPA.180103
Received: June 18, 2024 Revised: September 17, 2024 Accepted: December 22, 2024 Corrected: December 11, 2025