IoMT Security: SHA3-512, AES-256, RSA and LSB Steganography

Wassim Alexan, *SMIEEE*, Ahmed Ashraf
Eyad Mamdouh and Sarah Mohamed
Faculty of IET
The German University in Cairo
Cairo, Egypt
wassim.alexan@ieee.org

Mohamed Moustafa
Faculty of Informatics and Computer Science
The German International University in Cairo
Cairo, Egypt
mohamed.dawood@student.giu-uni.de

2021 8th NAFOSTED Conference on Information and Computer Science (NICS) | 978-1-6654-1001-4/21/$31.00 ©2021 IEEE | DOI: 10.1109/NICS54270.2021.9701567

***Abstract*—The Internet of Medical Things (IoMT) has been witnessing huge leaps in its development due to the advancements of neighboring technologies. Those include 5G, big data and cloud storage. While IoMT provides a rich environment for the ultra-fast share and transfer of pathological analyses and disease diagnoses, it also presents networking and security engineers with unprecedented challenges. The need to protect the transmission of the sensitive information in relation to patients' identities and diagnoses has always been a priority. This security problem is only exaggerated by the sheer volume of medical data to be transferred through a network in real time. This paper proposes an information security scheme for IoMT that utilizes AES-256, RSA, SHA3-512 and LSB embedding in medical scans or images. The proposed scheme not only guarantees the secure transmission of medical data through a network, but it also satisfies the conditions of user authentication and confidentiality. The numerical results showcase the superiority of the proposed scheme.**

***Keywords*–IoMT, AES, RSA, SHA, LSB.**

I. Introduction

Recent advances in Internet of Things (IoT) as well as persistent improvements medical devices and their connectivity to computer networks have lead to the conception of a new phenomenon, the Internet of Medical Things (IoMT). With rapid developments in this field and its near-ubiquity, concerns that relate to the security of IoMT are prevalent and quiet pressing. This is specifically true when it comes to securing the transmission of medical images among the different nodes on a network. Such medical images are generated from CT scans, fMRI, X-ray scans and many others. In many instances, such medical images are generated and automatically transmitted through the network without human intervention. However, either these images themselves or any of their related (directly printed on them) information are in many cases rather sensitive and need to be secured. To that end, various technologies attempt at providing such needed security. Those are classified into 2 major groups: cryptography and steganography. Cryptography is the simple act of expressing any sensitive information in the form of plaintext or plain images as illegible ciphertext or cipher images. The literature includes various examples, either directly related to IoMT security [1], [2] or to data encryption in general [3]. Steganography, however, is the act of concealing the existence of sensitive information in the first place. This is carried out through the secretive insertion of the sensitive information into multiple forms of cover media [4], [5]. The literature includes numerous techniques, once again, either directly related to IoMT security [6], [7] to data steganography in general [8], [9]. Furthermore, many research works include the combined utilization of both cryptography and steganography [10], [11]. What is rather notable in most of the aforementioned security schemes is that they do not take into account the importance of message and/or sender authentication [3]–[5], [8], [9], [11].

Medical images are widely popular in the medical community as their utilization helps in detecting, staging and treating different kinds of diseases in the organs of the human body. Medical images are becoming more vital in regular and advanced hospitals in diagnosing different kinds of anomalies [12]. In making use of medical scans, it is crucial to extract accurate information from them, as this helps in diagnosing the disease a patient is suffering from, and based on such diagnosis, the right treatment will be identified. Light conditions and limited exposure types can increase the chances of a noise appearing on a medical image, which affects the scan, leading to a false diagnosis. A noise changes the quality of an image to a low one which can lead to an inability to extract, analyze, recognize, and quantify the abnormality that is appearing in the image [12]. Medical image analysis is carried out by radiologists and physicians and is performed in special clinics [13]. Moreover, medical image analysis represents a crucial part of a patient's electronic records. Recently, the arising of telemedicine applications such as teleconsulting, telediagnosis, telesurgery, and others is due to the trading of medical images between hospitals and medical experts, such as radiologists and physicians. However, the data that is being exchanged needs to be secured as the trading is usually carried out in open communication channels which may raise the chances of manipulation and misappropriation [14].

In this research work, we propose a security scheme for IoMT applications. Our scheme involves the employment of a symmetric cryptography protocol, AES-256, as well as an asymmetric one, RSA. Furthermore, we make use of a hash algorithm, SHA3-512. Finally, the simple idea of LSB steganography is also employed. While we are well-aware of the availability of much more secure steganography schemes in the literature, some of which we developed

Authorized licensed use limited to: Univ of Calif Santa Cruz. Downloaded on March 12,2026 at 20:07:38 UTC from IEEE Xplore. Restrictions apply.

ourselves (as in [11], [15], [16]), we adopt simple LSB embedding with the sole purpose of illustrating its possible combination with the previously mentioned security standards (AES-256, RSA and SHA3-512). This paper is organized as follows. Section II describes the proposed security scheme. Section III presents the numerical results and showcases points of strength and robustness. Section IV draws the conclusions of the paper and suggests a future work.

II. The Proposed IoMT Security Scheme

A. Assumptions

In presenting our proposed scheme, we make a few assumptions. First of all, the IoMT under consideration is live, with massive amounts of sensitive data circulating between various nodes. Second, a symmetric encryption standard is available for use, namely AES-256, as well as an asymmetric encryption standard, namely RSA. Third, a hashing algorithm, namely SHA3-512 is employed. Note that while SHA2 is currently the hashing algorithm that is mostly adopted worldwide, SHA3-512 is the next generation of hashing algorithms and eventually will become the world standard [17]. This combination of AES256, RSA and SHA3-512 satisfies the CIA triad (confidentiality, integrity and availability) [17].

B. Implementation Steps

At the transmitter side: First, the sensitive medical information is hashed, utilizing SHA3-512. The output of the hash function is then encrypted with a private key, PR_a, utilizing RSA. Second, this encrypted data is concatenated with the plaintext data. Third, the concatenated data is encrypted with a symmetric key, k, utilizing AES-256. Next, this data is transformed into a bitstream. Fourth, this bitstream is LSB-embedded in the cover medical image, resulting in the stego medical image. Finally, this stego media is transmitted over the insecure channel (i.e the Internet).

At the receiver side: First, extraction of the LSB-embedded data is carried out. Second, the data is converted back into hexadecimal and decrypted utilizing the symmetric key, k of AES-256. Third, the data is split into 2 parts. One part is hashed, employing SHA3-512, while the other part is decrypted, employing the public key, PU_a, of RSA. Fourth, the outputs of the previous step are compared together.

Fig. 1 illustrates the steps of implementing the proposed IoMT security scheme.

III. Discussion of Features

A. Confidentiality

In essence, confidentiality means that only the sender and the receiver can read the plaintext data. In our proposed scheme this is achieved through the AES-256 encryption of the concatenation of the message data and the encrypted and hashed message data. Thus, even if an attacker sniffing the network intercepts our message, it becomes impossible to read the ciphertext, assuming that the attacker realizes there is embedded data in the medical image being transferred.

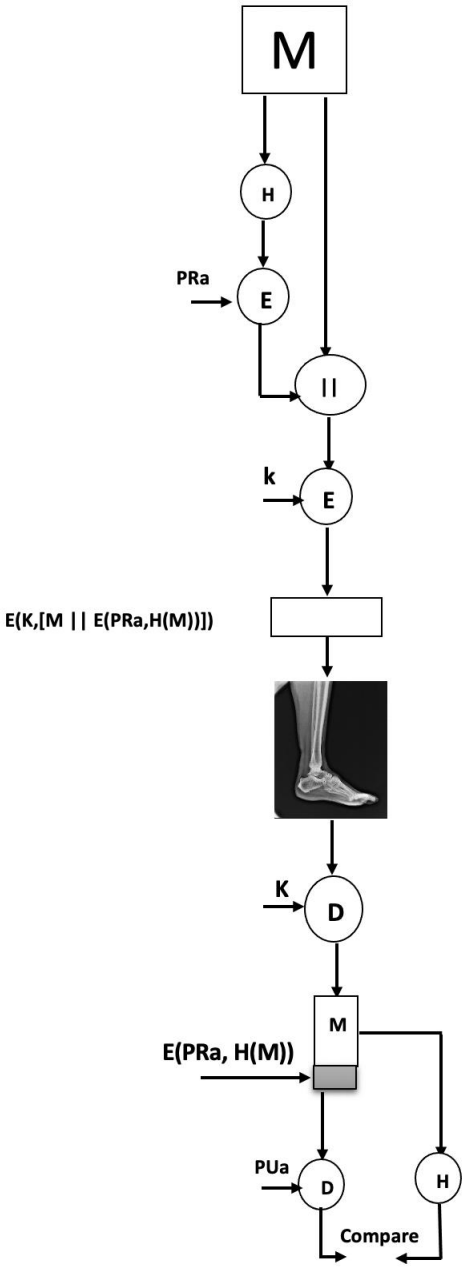


Fig. 1: Simplified flowchart of the proposed IoMT security scheme.

B. User Authentication

User authentication is about ensuring that the a message is indeed sent from the user claiming to have sent it, such that no other person can impersonate them. In our proposed scheme this is ensured through hashing the message data, then encrypting it using the sender's private key. While asymmetric encryption, or more specifically RSA, has many advantages, we are utilizing it here to verify user identity through digital signatures [18]. Every peer on the network has two keys, a public key that is know to all peers, and a private key known only to its owner. What is encrypted using the public key is could only be decrypted by the corresponding private key and vice versa. At the sender side, we are encrypting the hashed message with the sender's private key, which is only known to its owner (the sender). At the receiver side, the receiver will try to

Authorized licensed use limited to: Univ of Calif Santa Cruz. Downloaded on March 12,2026 at 20:07:38 UTC from IEEE Xplore. Restrictions apply.

decrypt the encrypted hashed message which is encrypted with the sender's private key. Now this message can only be decrypted using the corresponding public key. If the receiver is able to decrypt it successfully using the known sender's public key, then s/he is now positive that the peer s/he is communicating with is indeed the intended one, and not an attacker pretending to be the sender.

C. Integrity

Integrity or message authentication is achieved through the use of the cryptographic hashing function, SHA3-512. It is an algorithm which makes it computationally infeasible to find either: a) A data object that maps to a pre-specified hash result (the one-way property), or b) Two data objects that map to the same hash result (the collision-free property) [17]. Because of these properties, hashing functions are often used to determine whether or not data has been manipulated. For example, consider that an attacker attempts to perform a man in the middle (MITM) attack. This means that the attacker will intercept the message, read it, modify it, then resend it to the receiver (using replay attack, for example). In such a case, how can the receiver verify that the message has not been manipulated? Well, in our proposed scheme, the use of SHA3-512 solves such a problem. Since we hash our message then encrypt it using the sender's private key (for the sake of user authentication), then concatenate the plaintext message with the encrypted and hashed message, then finally encrypt the concatenated string with a symmetric key, this leads to the following situation. At the receiver side, first, s/he decrypts the whole block using the symmetric key. Then, splits the block into 2 parts. The first part is the plaintext message and the second part is the encrypted hashed message. S/he takes the part of the encrypted hashed message, decrypts it using the sender's public key (whereby user authentication is verified here) and in parallel, s/he takes the plaintext message and hashes it using the same hashing algorithm used in the sender side. Finally, s/he compares the 2 parts after these 2 parallel processes. If they are the same, then the message has not been manipulated.

IV. Numerical Results and Performance Evaluation

This section presents the experimental results of the proposed IoMT security scheme. The scheme's performance is evaluated against various metrics, over multiple test images. The proposed security scheme is implemented utilizing Wolfram Mathematica® on a computer with macOS Catalina v10.15.7, having a 2.9 GHz 6-Core Intel® Core™ i9 processor and 32 GB of 2400 MHz DDR4 of memory. Four medical images resulting from X-ray scans are employed in this section. These are shown in Table III. All images are resized to dimensions of 256×256.

An inspection of the images shown in Table III shows no visual differences between the cover and the stego X-ray scans. This is further tested through visually comparing their image histograms, which confirms the that no structural differences can be found through the human visual system (HVS).

TABLE I: Statistical performance metrics for image steganography.

Image	MSE	PSNR [dB]	H_c	H_s
Test 1	0.218216	54.7419	5.54518	5.54518
Test 3	0.213196	54.843	5.54518	5.54518
Test 12	0.215332	54.7997	5.54518	5.54518

TABLE II: Statistical performance metrics for image steganography.

Image	SSIM	NCC	Image Fidelity
Test 1	0.997774	0.999889	0.999969
Test 3	0.998058	0.999924	0.999989
Test 12	0.998255	0.99989	0.999974

A number of steganography performance evaluation metrics are computed and shown in Table I and Table II for the 3 test images. Table I shows that the MSE between the cover and the stego medical images is relatively small ($\sim$ 0.215). Correspondingly, this results in high PSNR values of over 54 dB. Moreover, Table I also shows the entropy values of the cover and stego medical images. Since entropy is a measure of information content in an image, and since the values do not change after embedding the sensitive data, this conveys a high level of security. Table II provides 3 more metrics, namely, the SSIM, the NCC and the image fidelity. Each of those metrics should be ideally equal to 1. With their values very close to the ideal, one can conclude once again that the proposed IoMT security scheme is effective at concealing the existence of the sensitive data.

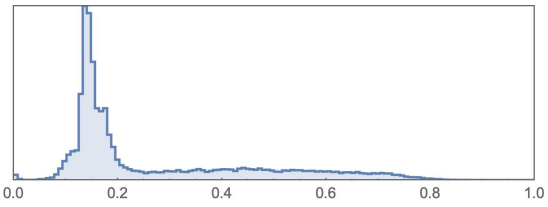
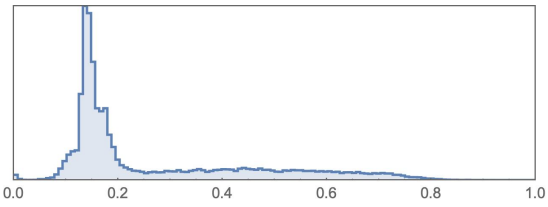
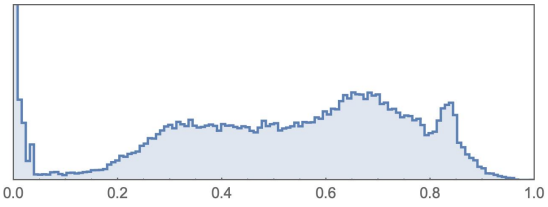
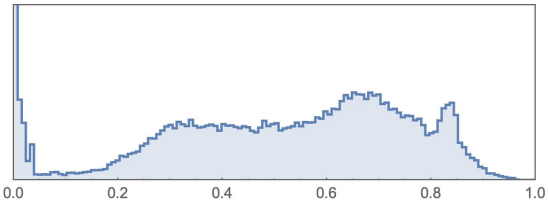
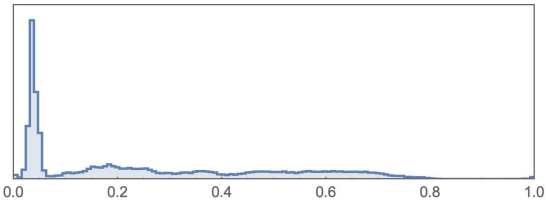
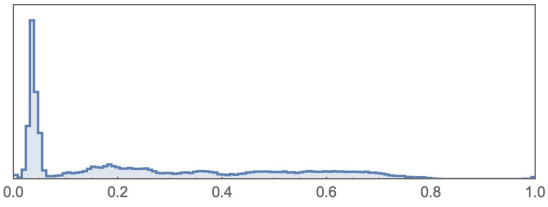
With low latency being a priority of any IoMT, a complexity analysis makes it clear whether or not a security scheme is appropriate for real time applications or not. Fig. 2 shows the time required for encryption and embedding, extraction and decryption, as well as the total time at both ends of the IoMT, against increasing number of sensitive data characters. Two observations can be made from Fig. 2. First and expectedly, as the number of characters increases, so does the processing time. Second, the total processing time required at both ends of an IoMT for the secure transmission of over 5000 characters is less than 1s.

V. Conclusions and Future Works

In this work, we proposed an IoMT security scheme to protect patients' information or records that accompany images resulting from medical scans such as X-rays. The proposed scheme employed AES-256, RSA, SHA3-512 and LSB embedding in medical scans or images. Our proposed scheme not only guarantees the secure transmission of such medical data through insecure channels or networks, but also satisfies the conditions of user authentication and confidentiality. Future works could

Authorized licensed use limited to: Univ of Calif Santa Cruz. Downloaded on March 12,2026 at 20:07:38 UTC from IEEE Xplore. Restrictions apply.

TABLE III: Numerical results of the achieved values for various metrics.

Image data	Cover image/histogram	Stego image/histogram
Test 1 $d = 256 \times 256$	 	 
Test 3 $d = 256 \times 256$	 	 
Test 12 $d = 256 \times 256$	 	 

Authorized licensed use limited to: Univ of Calif Santa Cruz. Downloaded on March 12,2026 at 20:07:38 UTC from IEEE Xplore. Restrictions apply.

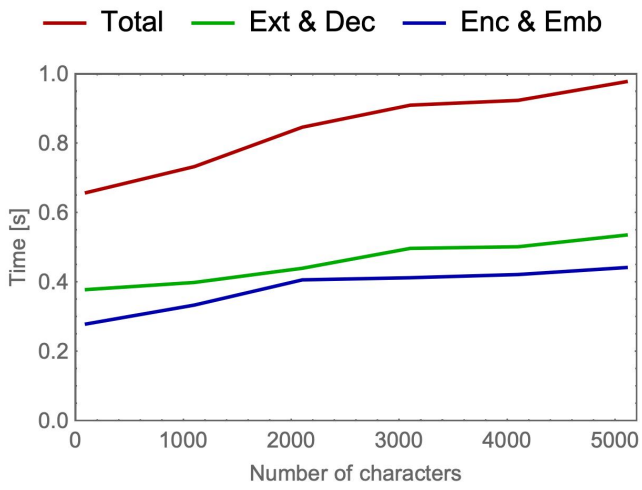


Fig. 2: Time complexity of the proposed security scheme.

include a similar approach, however, one that utilizes 3D models generated from medical scans (e.g. fMRI or CT scans).

REFERENCES

[1] A. Ghubaish, T. Salman, M. Zolanvari, D. Unal, A. Al-Ali, and R. Jain, "Recent advances in the internet-of-medical-things (iomt) systems security," *IEEE Internet of Things Journal*, vol. 8, no. 11, pp. 8707–8718, 2021.

[2] G. Hatzivasilis, O. Soultatos, S. Ioannidis, C. Verikoukis, G. Demetriou, and C. Tsatsoulis, "Review of security and privacy for the internet of medical things (iomt)," in *2019 15th International Conference on Distributed Computing in Sensor Systems (DCOSS)*, 2019, pp. 457–464.

[3] M. T. Elkandoz, W. Alexan, and H. H. Hussein, "Logistic sine map based image encryption," in *2019 Signal Processing: Algorithms, Architectures, Arrangements, and Applications (SPA)*, 2019, pp. 290–295.

[4] F. Hemeida, W. Alexan, and S. Mamdouh, "A comparative study of audio steganography schemes," *International Journal of Computing and Digital Systems*, vol. 10, pp. 555–562, 2021.

[5] W. Alexan and F. Hemeida, "Security through blowfish and lsb bit–cycling with mathematical sequences," in *2019 Signal Processing: Algorithms, Architectures, Arrangements, and Applications (SPA)*. IEEE, 2019, pp. 229–234.

[6] S. Gull, S. A. Parah, and K. Muhammad, "Reversible data hiding exploiting huffman encoding with dual images for iomt based healthcare," *Computer Communications*, vol. 163, pp. 134–149, 2020.

[7] S. Devi, M. N. Sahoo, K. Muhammad, W. Ding, and S. Bakshi, "Hiding medical information in brain mr images without affecting accuracy of classifying pathological brain," *Future Generation Computer Systems*, vol. 99, pp. 235–246, 2019.

[8] M. T. Elkandoz, W. Alexan, and H. H. Hussein, "3d image steganography using sine logistic map and 2d hyperchaotic map," in *2019 International Conference on Electrical and Computing Technologies and Applications (ICECTA)*. IEEE, 2019, pp. 1–6.

[9] S. Farrag and W. Alexan, "Secure 3d data hiding technique based on a mesh traversal algorithm," *Multimedia Tools and Applications*, vol. 79, no. 39, pp. 29 289–29 303, 2020.

[10] H. T. ALRikabi and H. T. Hazim, "Enhanced data security of communication system using combined encryption and steganography." *International Journal of Interactive Mobile Technologies*, vol. 15, no. 16, 2021.

[11] Y. Moussa and W. Alexan, "Message security through aes and lsb embedding in edge detected pixels of 3d images," in *2020 2nd Novel Intelligent and Leading Emerging Sciences Conference (NILES)*. IEEE, 2020, pp. 224–229.

[12] B. Goyal, S. Agrawal, and B. Sohi, "Noise issues prevailing in various types of medical images," *Biomedical & Pharmacology Journal*, vol. 11, no. 3, p. 1227, 2018.

[13] D. Shen, G. Wu, and H.-I. Suk, "Deep learning in medical image analysis," *Annual review of biomedical engineering*, vol. 19, pp. 221–248, 2017.

[14] A. Al-Haj, "Providing integrity, authenticity, and confidentiality for header and pixel data of dicom images," *Journal of digital imaging*, vol. 28, no. 2, pp. 179–187, 2015.

[15] S. Farrag, W. Alexan, and H. H. Hussein, "Triple-layer image security using a zigzag embedding pattern," in *2019 International Conference on Advanced Communication Technologies and Networking (CommNet)*. IEEE, 2019, pp. 1–8.

[16] S. Farrag and W. Alexan, "Secure 2d image steganography using recamán's sequence," in *2019 International Conference on Advanced Communication Technologies and Networking (CommNet)*. IEEE, 2019, pp. 1–6.

[17] W. Stallings, *Cryptography and network security, 4/E*. Pearson Education India, 2006.

[18] P. Kumar and S. K. Sharma, "An empirical evaluation of various digital signature scheme in wireless sensor network," *IETE Technical Review*, pp. 1–11, 2021.

Authorized licensed use limited to: Univ of Calif Santa Cruz. Downloaded on March 12,2026 at 20:07:38 UTC from IEEE Xplore. Restrictions apply.