

Techniques of medical image encryption taxonomy

Mustafa A. Al-Fayoumi¹, Ammar Odeh¹, Ismail Keshta², Ashraf Ahmad¹

¹Department of Computer Science, Princess Sumaya University for Technology, Amman, Jordan

²Department of Computer Science and Information Systems, College of Applied Sciences, AlMaarefa University, Riyadh, Saudi Arabia

Article Info

Article history:

Received Mar 24, 2022

Revised May 16, 2022

Accepted Jun 9, 2022

Keywords:

Digital medical images

Genetic algorithms

Internet of medical things

S-box

ABSTRACT

Medical images are one of the most significant and sensitive data types in computer systems. Sending medical images over the internet necessitates using a robust encryption scheme that is resistant to cryptographic attacks. Confidentiality is the most critical part of the three security objectives for information systems security, namely confidentiality, integrity, and availability. Confidentiality is the most critical aspect for the secure storage and transfer of medical images. In this study, we attempt to classify various encryption methods in order to assist researchers in selecting the optimal strategy for protecting sensitive patient information while transferring medical images without alteration and outline the measures that should be adopted to address challenges and concerns relevant to techniques of medical image encryption.

This is an open access article under the [CC BY-SA](#) license.



Corresponding Author:

Ammar Odeh

Department of Computer Science, King Hussein School of Computing Sciences, Princess Sumaya

University for Technology (PSUT) Al-Jubaiha

Amman, Jordan

Email: a.odeh@psut.edu.jo

1. INTRODUCTION

The need for content protection for digital medical images is growing, especially with the advancement of computerized systems and communication networks that enable high-quality images to be sent and received in real-time [1], [2]. Healthcare organizations must encrypt all patient data, such as photographs, before moving it over computer networks due to medical concerns. As a result, researching and improving certified encryption algorithms is crucial in modern medicine [3]. Medical image encryption techniques attempt to convert a digital image to a different image data format that is difficult to recognize [4]-[7].

It's difficult to overestimate the relevance of image security in the field of medical imaging. Several studies have been carried out to ensure the security of medical healthcare photographs [8]. Encryption is the best method for image confidentiality since it prevents data loss. Traditional encryption solutions cannot be directly applied to e-health data because of data size limits, redundancy, and capacity, especially when patient data is sent via open channels [9]. As a result, patients may lose the privacy of their data contents, as images differ from text due to their two distinct causes of data loss and confidentiality. Researchers have recognized similar security vulnerabilities and offered several picture encryption solutions to address the issue [10]-[12].

The volume of various medical images has recently exploded due to the emergence of new technology in medical sectors [13], [14], such as high-quality imaging instruments, fast and accurate computing systems, and dependable communication networks [15], [16]. Effective image encryption approaches for medical image content protection have become more significant, and there are currently several robust encryption algorithms available to secure both two-dimensional (2D) and three-dimensional (3D) medical images [17]-[19]. From a technological standpoint, the created technique can be divided into frequency domain encryption, and spatial domain encryption approaches, with low-level and high-level

methods for each [20], [21]. While the content of the image remains understandable and visible when using low-level image encryption algorithms, the image's content will be completely disordered, and the content of the original photos will be invisible when utilizing high-level image encryption techniques [22].

Healthcare organizations and hospitals should strike a balance between the benefits that the internet of medical things (IoMT) offers and ensure that they have the necessary protocols and policies to address the security risks it poses [23], [24]. Consumer health monitoring innovations such as the Nike Fuel band, Fit Bit, or Withings monitor an individual's health or a specific fitness regimen and connect to multiple mobile systems utilizing Bluetooth innovation are examples of IoMT [25], [26]. Figure 1 shows the encryption model for a medical image considered plain text; the sender and receiver agreed on the secret key and the encryption algorithm to encrypt the image to produce the cipher image.

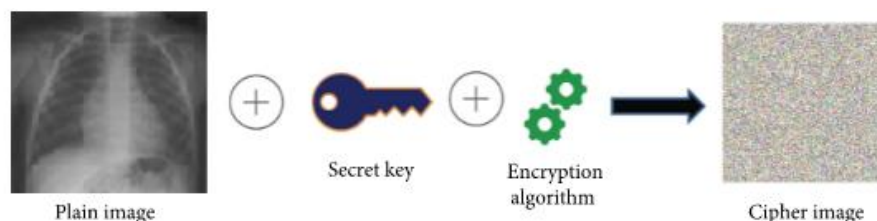


Figure 1. Medical image and the corresponding encrypted image

2. DATA COLLECTION PROCESS

The researcher did a literature search to identify types of medical data encryption and the relevant challenges and concerns. The secondary sources that were deemed appropriate comprised books, articles, and periodicals that had content on medical data encryption and trust challenges and concerns. The researcher searched various articles from different databases like Google Scholars, ERIC, EBSCOhost, and PubMed. The general search process used different keywords such as encryption, data, and medical images. Papers and articles were picked from the relevant search results as long as the respective article met the relevant inclusion criteria [27].

More specifically, the search approach used in various organization databases yielded roughly 4450 records, which included traditional research studies as well as reports from other health organizations. Despite the fact that the search method made a considerable amount of data available, the data cleaning process was used to remove all relevant duplicates. After removing all duplicates, there were only 2765 articles left. As a result, the abstracts and titles of these papers were scrutinized to see if they satisfied the other relevant inclusion criteria. As a result of the overall research methods and designs, more studies were omitted. The search results are depicted in the PRISMA research flowchart as shown in Figure 2 (see in appendix).

3. SECURITY PRINCIPLES

Medical image security is built on confidentiality, trustworthiness, privacy, authenticity, and integrity. Medical images in modern digital imaging systems are typically large in size and have a high level of redundancy [28], [29]. For intelligent healthcare and image cloud systems, real-time and resource-constrained security methods are required, and traditional algorithms cannot meet these requirements. As a result, a slew of new algorithms have arisen, all of which are examined [30]-[32]. Figure 3 presents the main five security principles that take on the encryption purpose.

3.1. Confidentiality

A storage or transmission application can be provided with confidentiality in two ways. For starters, the underlying computing architecture provides means for maintaining confidentiality. Complete transparency is a benefit. The obvious downside is that all programs are given confidentiality regardless of whether they are required or not. It is not feasible to utilize the unique qualities of specific applications. On the application layer, the second approach is to provide confidentiality. Only apps and services with a need for confidentiality are protected here [33].

The issue is that each application is responsible for its own confidentiality; the benefit is that unique properties of some apps may be used to build more efficient encryption schemes, or encryption can be disabled if it is not required [34]. The second type of encryption is selective encryption of medical picture data, which takes advantage of the redundancy of visual data [35].

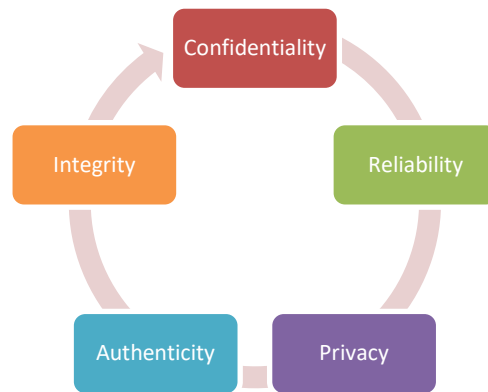


Figure 2. Security principles

3.2. Reliability

Medical image dependability is a prerequisite for intelligent healthcare implementation. The security of the medical image cloud platform and the dependability of the image source are critical needs for image cloud systems, and they're a must-have for anyone building a cloud image system. As a result, to ensure the safe transmission and storage of images, the medical image security algorithm must have a strong anti-attack capability [36], [37].

3.3. Privacy

The patient's privacy and personal information are involved in the medical image, which cannot be freely disclosed or stolen. It must not be abused or overused; otherwise, it would result in significant losses for the government and individuals and irreversible harm [38]. The necessity for privacy is an incredibly crucial part of medical image security, and it should be considered first while researching security algorithms [39].

3.5. Integrity

There are usually many medical photographs for a patient or a disease scenario. Different information will be available at different phases of the diagnosis and therapy process. Medical images should be guaranteed to be comprehensive and dependable when they are transmitted and stored remotely. As a result, implementing multi-image fusion encryption and multiple information concealment in security techniques is essential [40].

4. RESULTS RELATED WORK

A new solution for grayscale medical picture protection is proposed in [41], Genetic algorithms are based on their qualities. Several of the algorithm's processes (population, crossover, and mutation) are key-dependent, and the recurrence of crossover and mutation processes improves the algorithm's robustness. The results of the rigorous security analysis (correlation coefficient, entropy, NPCR, key sensitivity, MSE, and so on) demonstrate the robustness of the proposed method, indicating that the proposed scheme has a high order of security and can thus be used for real-time transmission of digital grayscale medical images.

Çavuşoğlu *et al.* [42] introduced a novel secure image encryption technique based on a new chaos-based RNG and S-BOX structure. S-Box, one of the most fundamental components of block encryption methods, is used in the latest encryption technique. First and foremost, the new chaotic system is introduced, followed by analyses. Analyses of the system found that it had sufficiently complicated dynamic properties. NIST tests for random bit sequence of three phases from the RNG are performed after the chaotic system is placed into the RNG. An RNG design that produces bit series that meet all NIST standards is thought to be capable of generating random bits from an encryption method. Bit series from the x and z phases of the RNG are utilized to generate chaos-based S-BOX for use in encryption algorithm design and S-box generating algorithm.

The encryption and decryption technique created here is used to encrypt and decrypt images. Encryption and decryption operations are done solely with chaos-based and AES algorithms to determine the security and performance level of the generated encryption algorithm.

Banik *et al.* [43] proposed a novel elliptic curve equivalent of the ElGamal cryptosystem. The proposed algorithm encrypts any Cartesian space coordinate, constrained by positive modulo p . Multiple

pixel values were base converted and fed as Pm directly without expressing them as discrete Elliptic Curve coordinates, which aids in data expansion reduces the amount of elliptic curve mathematical operations. Furthermore, the discovery contributes to a significant increase in execution speed.

The simple image's 512-bit hash value is used in [44] to generate one-time starting conditions for a four-wing complex chaotic system-based asymmetric color picture encryption scheme. Three pairs of chaotic sequences are used to encrypt the pixels of the red, green, and blue components of the odd and even number indices.

Dai *et al.* proposed in [45] a chaotic picture encryption approach based on bit-plane decomposition. The ciphertext image is first split into an eight-bitmap, with the top four bits accounting for a significant amount of plain text. As a result, Arnold permutation on the high four-bit is used to correlate the time of permutation with the image order. After then, the scrambled images are combined to form a new scrambled image, which is then discussed. Henon maps are used to enhance the argument process. Henon mapping parameters were obtained by iterating the logistic map N times. Two Henon mapping sequences split two into four, which were then mixed into scrambled images and ciphertext images using the XOR technique.

Mitra *et al.* [46] described a method for encrypting images using a random permutations mix; using a combination of several permutations approaches, this research proposes a simple-to-implement yet effective solution for image encryption. The primary notion is that the visual information in an image can be minimized by reducing the association between bits, pixels, and blocks using particular permutation techniques.

The suggested method [47] uses a coupled map lattice to build an initial population of secure cipher-images for MGA. The MGA is then used to improve the entropy of the cipher-images while reducing the algorithm's computing time. Experiments and computer simulations show that the proposed solution, which uses a hybrid algorithm, provides excellent encryption and resists a variety of common assaults.

5. EVALUATION METRICS

Most of the previous research worked on maintaining the confidentiality of patient information and measuring this through various criteria to prove the ability to encrypt and decrypt medical images at high speed and without changing the content of the image, and accordingly, the following criteria were agreed upon. Color palette a color space is a collection of colors that has been organized in a specific way. It aids repeatable color representations, whether the model is an analog or digital image, when used in conjunction with color profiling enabled by various physical instruments.

The time it takes for an encryption process to generate a ciphertext from plaintext is known as the encryption time. Encryption time is used to calculate an encryption technique's throughput. It refers to the speed with which data is encrypted. Entropy is defined in images as the equivalent states of intensity level to which individual pixels can adapt. The average uncertainty of the information source is interpreted as entropy, which is a measure of image information content.

$$H(s) = \sum_{i=0}^{2^n-1} P(s_i) \log_2 \frac{1}{P(s_i)} \quad (1)$$

The correlation coefficient factor is used in security analysis to quantify the link between plaintext and encryption variables. As a result, the ciphertext must be distinct from the plaintext.

$$P_{xy} = \frac{\text{cov}(x,y)}{\sigma_x \sigma_y} \quad (2)$$

Table 1 shows the comparison among seven algorithms to encrypt medical images; most of the proposed algorithms used the Grayscale image. [41] introduced the fastest encryption time and excellent entropy value of 7.99. In the case of color images, the [44] shows a high-performance encryption time.

Table 1. Evaluation metrics comparison

Ref	Color space	Image size	encryption time (s)	Entropy	correlation coefficient
[41]	Grayscale	512*512	00.35	7.99	0.00136
[42]	Grayscale	512*513	2.382	7.9559	0.531
[43]	grayscale	512*514	0.5	7.89	0.00116
[44]	RGB	512*515	5.9	7.9886	0.001197
[45]	grayscale	512*516	1.33	7.88	0.00012
[46]	grayscale	512*517	1.759	7.87	0.00133
[47]	grayscale	257 × 256	2.35	7.93	0.0097

6. FUTURE SCOPE

Medical images are considered among the most sensitive and significant groups of data. Sharing medical images through the internet necessitates the application of a robust encryption scheme that is resistant to any form of attack. Several techniques of medical image encryption, such as watermarking and algorithm passwords, have been used widely in the clinical support system to protect medical images from unauthorized users. A comprehensive knowledge base and advanced functionalities are essential in designing efficient encryption methods for medical images. Despite the advanced knowledge on numerous encryption methods of medical images, strict security and confidentiality challenges and concerns are still linked to such data. For instance, hackers can still intrude on encrypted medical images and use such images without the patient's written permission.

To achieve the maximum level of privacy and secrecy on medical data, the security and privacy problems related with encrypted medical images must be addressed permanently. To begin, it's critical to understand that data encryption employs a variety of technologies, protocols, and services to achieve a specific aim. To obtain the intended result, it is critical to establish a set of rules that must be followed at all stages of medical picture encryption, from the micro to the macro. The current criteria for medical picture encryption are a set of architecture standards that comprise interfaces, data models, and appropriate protocols that can handle a wider range of devices, humans, operating systems, and languages. This will prevent an unauthorized person from gaining access to all of the encrypted medical image data. Hackers can readily break most encryption methods, such as watermark and password algorithms, as previously stated.

Second, identity management is required to address both the security and privacy issues associated with incorrect data utilization or encryption. Within the internet of things, identity management can be accomplished by attempting to share identifying pertinent information between devices for all first-time connections. Such a method is vulnerable to eavesdropping, which can result in a man-in-the-middle assault, jeopardizing the entire framework of medical picture encryption. As a result, there are some critical requirements for a form of preconfigured identity or hub management entity that can monitor the overall connection process of relevant devices using encryption and other relevant approaches to help prevent identity theft.

The three-layer design of medical image encryption, according to most authors, never allows for the actual opening, closure, and adequate management of a session between the two items. As a result, protocols are desperately needed to handle all of these challenges and, eventually, to make communication between the essential devices easier. There is a pressing need for an abstract session layer to be included as an additional layer within encrypted data.

7. CONCLUSION

Medical photographs are among the most sensitive and important types of information. Sharing medical photos over the internet needs the use of a robust encryption technique that is impregnable to assault. Confidentiality is one of the most important aspects of any information security system, which includes availability, integrity, and confidentiality. Confidentiality is a critical feature of the secure sharing and storage of pertinent medical pictures. However, the most pressing challenge in achieving everlasting anonymity on medical photographs is security. If security considerations such as confidentiality, privacy, access control, authentication, end-to-end security, trust management, worldwide standards, and applicable policies are properly addressed, nearly anything in the healthcare sector, particularly medical imaging, can be transformed. New wireless identification, software, and hardware technologies are desperately needed to address all of the privacy and security issues that come with encrypted data.

ACKNOWLEDGEMENTS

The authors sincerely acknowledge the Princess Sumaya University for Technology and the Researchers Supporting Program (TUMA-Project-2021-14), AlMaarefa University, Riyadh, Saudi Arabia, for supporting steps of this work.

APPENDIX

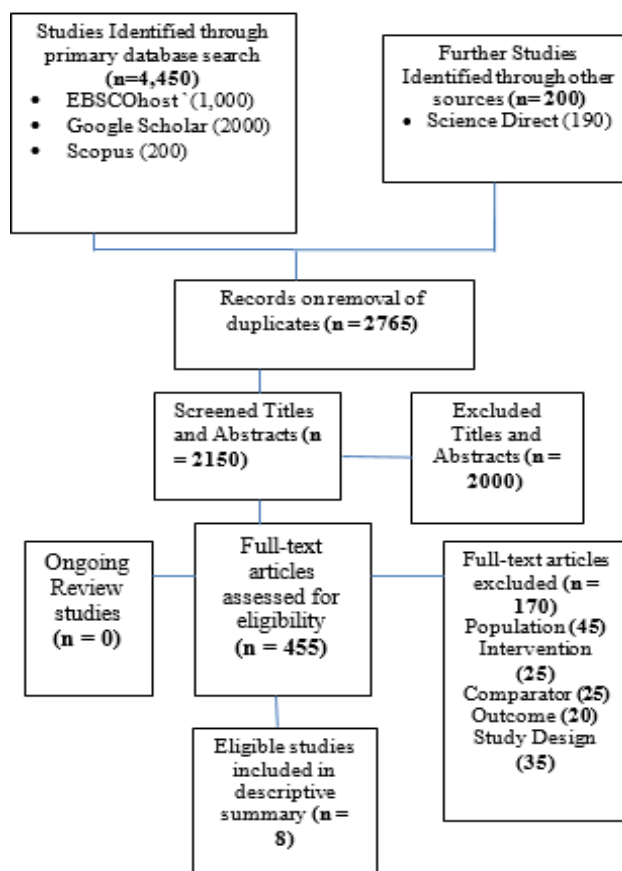





Figure 3. Flowchart of search results from the PRISMA study

REFERENCES




- [1] J. Li *et al.*, "A partial encryption algorithm for medical images based on quick response code and reversible data hiding technology," *BMC Medical Informatics and Decision Making*, vol. 20, p. 297, 2020, doi: 10.1186/s12911-020-01328-2.
- [2] L. Faes *et al.*, "Automated deep learning design for medical image classification by health-care professionals with no coding experience: a feasibility study," *The Lancet Digital Health*, vol. 1, pp. e232-e242, 2019, doi: 10.1016/S2589-7500(19)30108-6.
- [3] R. R. Paulsen and T. B. Moeslund, *Introduction to medical image analysis*, Switzerland: Springer Nature, 2020.
- [4] F. Masood *et al.*, "A lightweight chaos-based medical image encryption scheme using random shuffling and XOR operations," *Wireless Personal Communications*, 2021, doi: 10.1007/s11277-021-08584-z.
- [5] Y. Pourasad, R. Ranjbarzadeh, and A. Mardani, "A new algorithm for digital image encryption based on chaos theory," *Entropy*, vol. 23, no. 3, p. 341, 2021, doi: 10.3390/e23030341.
- [6] M. Begum and M. S. Uddin, "Digital image watermarking techniques: a review," *Information*, vol. 11, no. 2, p. 110, 2020, doi: 10.3390/info11020110.
- [7] A. Odeh, I. Keshta and E. Abdelfattah, "Machine Learning Techniques for Detection of Website Phishing: A Review for Promises and Challenges," *2021 IEEE 11th Annual Computing and Communication Workshop and Conference (CCWC)*, 2021, pp. 0813-0818, doi: 10.1109/CCWC51732.2021.9375997.
- [8] T. Poletto, M. M. Silva, T. R. N. Clemente, A. P. H. de Gusmão, A. P. d. B. Araújo, and A. P. C. S. Costa, "A Risk Assessment Framework Proposal Based on Bow-Tie Analysis for Medical Image Diagnosis Sharing within Telemedicine," *Sensors*, vol. 21, no. 7, p. 2426, 2021, doi: 10.3390/s21072426.
- [9] H. Ayesha *et al.*, "Automatic medical image interpretation: State of the art and future directions," *Pattern Recognition*, vol. 114, p. 107856, 2021, doi: 10.1016/j.patcog.2021.107856.
- [10] M. J. Willemink *et al.*, "Preparing medical imaging data for machine learning," *Radiology*, vol. 295, no. 1, pp. 4-15, 2020, doi: 10.1148/radiol.2020192224.
- [11] Q. Duan *et al.*, "SenseCare: A research platform for medical image informatics and interactive 3D visualization," arXiv preprint arXiv:2004.07031, 2020, doi: 10.48550/arXiv.2004.07031.
- [12] B. P. Battula and B. Duraisamy, "Medical Image Data Classification Using Deep Learning Based Hybrid Model with CNN and Encoder," *Rev. d'Intelligence Artif.*, vol. 34, no. 5, pp. 645-652, 2020, doi: 10.18280/ria.340516.
- [13] S. P. Singh, L. Wang, S. Gupta, H. Goli, P. Padmanabhan, and B. Gulyás, "3D deep learning on medical images: a review," *Sensors*, vol. 20, no. 18, p. 5097, 2020, doi: 10.3390/s20185097.
- [14] P. Savadjiev *et al.*, "Demystification of AI-driven medical image interpretation: past, present and future," *European radiology*, vol. 29, no. 3, pp. 1616-1624, 2019, doi: 10.1007/s00330-018-5674-x.

- [15] A. Alexander, M. McGill, A. Tarasova, C. Ferreira, and D. Zurkiya, "Scanning the future of medical imaging," *Journal of the American College of Radiology*, vol. 16, no. 4, pp. 501-507, 2019, doi: 10.1016/j.jacr.2018.09.050.
- [16] S. B. Atitallah, M. Driss, W. Boulila, and H. B. Ghézala, "Leveraging Deep Learning and IoT big data analytics to support the smart cities development: Review and future directions," *Computer Science Review*, vol. 38, p. 100303, 2020, doi: 10.1016/j.cosrev.2020.100303.
- [17] P. Galetsi, K. Katsaliaki, and S. Kumar, "Big data analytics in health sector: Theoretical framework, techniques and prospects," *International Journal of Information Management*, vol. 50, pp. 206-216, 2020, doi: 10.1016/j.ijinfomgt.2019.05.003.
- [18] L. Cai, J. Gao, and D. Zhao, "A review of the application of deep learning in medical image classification and segmentation," *Annals of translational medicine*, vol. 8, no. 11, p. 713, 2020, doi: 10.21037/atm.2020.02.44.
- [19] A. Odeh, A. Alarbi, I. Keshta, and E. Abdelfattah, "Efficient prediction of phishing websites using multilayer perceptron (MLP)," *Journal of Theoretical and Applied Information Technology*, vol. 98, no. 16, pp. 3353-3363, 2020.
- [20] A. Banu S and R. Amirtharajan, "A robust medical image encryption in dual domain: chaos-DNA-IWT combined approach," *Medical & Biological Engineering & Computing*, vol. 58, pp. 1445-1458, 2020, doi: 10.1007/s11517-020-02178-w.
- [21] O. S. Faragallah et al., "Investigation of Chaotic Image Encryption in Spatial and FrFT Domains for Cybersecurity Applications," *IEEE Access*, vol. 8, pp. 42491-42503, 2020, doi: 10.1109/ACCESS.2020.2974226.
- [22] H. M. Ghadirli, A. Nodehi, and R. Enayatifar, "An overview of encryption algorithms in color images," *Signal Processing*, vol. 164, pp. 163-185, 2019, doi: 10.1016/j.sigpro.2019.06.010.
- [23] F. Al-Turjman, M. H. Nawaz, and U. D. Ulusar, "Intelligence in the Internet of Medical Things era: A systematic review of current and future trends," *Computer Communications*, vol. 150, pp. 644-660, 2020, doi: 10.1016/j.comcom.2019.12.030.
- [24] A. Odeh, I. Keshta, A. Aboshgifa and E. Abdelfattah, "Privacy and Security in Mobile Health Technologies: Challenges and Concerns," *2022 IEEE 12th Annual Computing and Communication Workshop and Conference (CCWC)*, 2022, pp. 0065-0071, doi: 10.1109/CCWC54503.2022.9720863.
- [25] R. P. Singh, M. Javaid, A. Haleem, R. Vaishya, and S. Ali, "Internet of Medical Things (IoMT) for orthopaedic in COVID-19 pandemic: Roles, challenges, and applications," *Journal of Clinical Orthopaedics and Trauma*, vol. 11, no. 4, pp. 713-717, 2020, doi: 10.1016/j.jcot.2020.05.011.
- [26] S. Vishnu, S. R. J. Ramson and R. Jegan, "Internet of Medical Things (IoMT) - An overview," *2020 5th International Conference on Devices, Circuits and Systems (ICDCS)*, 2020, pp. 101-104, doi: 10.1109/ICDCS48716.2020.2435558.
- [27] A. Odeh, K. Elleithy, and M. Faezipour, "A Reliable and Fast Real-Time Hardware Engine for Text Steganography," *IEEE LISAT 2014 Long Island Systems, Applications and Technology*, pp. 1-6, 2014.
- [28] T. Yaqoob, H. Abbas and M. Atiquzzaman, "Security Vulnerabilities, Attacks, Countermeasures, and Regulations of Networked Medical Devices—A Review," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 4, pp. 3723-3768, Fourthquarter 2019, doi: 10.1109/COMST.2019.2914094.
- [29] J. T. J. Penttinen, *5G explained: security and deployment of advanced mobile communications*, New York: John Wiley & Sons, 2019.
- [30] L. Abualigah, A. Diabat, P. Sumari and A. H. Gandomi, "Applications, Deployments, and Integration of Internet of Drones (IoD): A Review," *IEEE Sensors Journal*, vol. 21, no. 22, pp. 25532-25546, 15 Nov.15, 2021, doi: 10.1109/JSEN.2021.3114266.
- [31] M. N. Mahdi, A. R. Ahmad, Q. S. Qassim, H. Natiq, M. A. Subhi, and M. Mahmoud, "From 5G to 6G technology: meets energy, internet-of-things and machine learning: a survey," *Applied Sciences*, vol. 11, no. 17, p. 8117, 2021, doi: 10.3390/app11178117.
- [32] D. Oladimeji, "An Intrusion Detection System for Internet of Medical Things," M.S. thesis, Dalhousie University, 2021.
- [33] R. Yang, F. R. Yu, P. Si, Z. Yang and Y. Zhang, "Integrated Blockchain and Edge Computing Systems: A Survey, Some Research Issues and Challenges," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 2, pp. 1508-1532, Secondquarter 2019, doi: 10.1109/COMST.2019.2894727.
- [34] W. B. Issa et al., "Privacy, confidentiality, security and patient safety concerns about electronic health records," *International Nursing Review*, vol. 67, no. 2, pp. 218-230, 2020, doi: 10.1111/inr.12585.
- [35] G. Wang, R. Lu, and Y. L. Guan, "Achieve Privacy-Preserving Priority Classification on Patient Health Data in Remote eHealthcare System," *IEEE Access*, vol. 7, pp. 33565-33576, 2019, doi: 10.1109/ACCESS.2019.2891775.
- [36] M. A. Sujan, D. Embrey, and H. Huang, "On the application of human reliability analysis in healthcare: opportunities and challenges," *Reliability Engineering & System Safety*, vol. 194, p. 106189, 2020, doi: 10.1016/j.res.2018.06.017.
- [37] A. Shamayleh, M. Awad, and A. O. Abdulla, "Criticality-based reliability-centered maintenance for healthcare," *Journal of Quality in Maintenance Engineering*, vol. 26 no. 2, pp. 311-334, 2019, doi: 10.1108/JQME-10-2018-0084.
- [38] A. Fourcade and R. Khonsari, "Deep learning in medical image analysis: A third eye for doctors," *Journal of stomatology, oral and maxillofacial surgery*, vol. 120, no. 4, pp. 279-288, 2019, doi: 10.1016/j.jormas.2019.06.002.
- [39] M. Shen, Y. Deng, L. Zhu, X. Du, and N. Guizani, "Privacy-Preserving Image Retrieval for Medical IoT Systems: A Blockchain-Based Approach," *IEEE Network*, vol. 33, no. 5, pp. 27-33, Sept.-Oct. 2019, doi: 10.1109/MNET.001.1800503.
- [40] A. Al Omar, M. Z. A. Bhuiyan, A. Basu, S. Kiyomoto, and M. S. Rahman, "Privacy-friendly platform for healthcare data in cloud based on blockchain environment," *Future generation computer systems*, vol. 95, pp. 511-521, 2019, doi: 10.1016/j.future.2018.12.044.
- [41] N. K. Pareek and V. Patidar, "Medical image protection using genetic algorithm operations," *Soft Computing*, vol. 20, pp. 763-772, 2016, doi: 10.1007/s00500-014-1539-7.
- [42] Ü. Çavuşoğlu, S. Kaçar, I. Pehlivan, and A. Zengin, "Secure image encryption algorithm design using a novel chaos based S-Box," *Chaos, Solitons & Fractals*, vol. 95, pp. 92-101, 2017, doi: 10.1016/j.chaos.2016.12.018.
- [43] A. Banik, Z. Shamsi, and D. S. Laiphrakpam, "An encryption scheme for securing multiple medical images," *Journal of Information Security and Applications*, vol. 49, p. 102398, 2019, doi: 10.1016/j.jisa.2019.102398.
- [44] H. Liu, A. Kadir, and Y. Li, "Asymmetric color pathological image encryption scheme based on complex hyper chaotic system," *Optik*, vol. 127, no. 15, pp. 5812-5819, 2016, doi: 10.1016/j.ijleo.2016.04.014.
- [45] Y. Dai, H. Wang, and Y. Wang, "Chaotic medical image encryption algorithm based on bit-plane decomposition," *International Journal of Pattern Recognition and Artificial Intelligence*, vol. 30, no. 4, p. 1657001, 2016, doi: 10.1142/S0218001416570019.
- [46] A. Mitra, Y. S. Rao, and S. Prasanna, "A new image encryption approach using combinational permutation techniques," *International Journal of Computer Science*, vol. 1, no. 2, pp. 127-131, 2006.
- [47] H. Nematzadeh, R. Enayatifar, H. Motameni, F. G. Guimarães, and V. N. Coelho, "Medical image encryption using a hybrid model of modified genetic algorithm and coupled map lattices," *Optics and Lasers in Engineering*, vol. 110, pp. 24-32, 2018, doi: 10.1016/j.optlaseng.2018.05.009.




BIOGRAPHIES OF AUTHORS

Mustafa A. Al-Fayoumi    received a BSc degree in Computer Science from Yarmouk University, Irbid, Jordan, in 1988. He earned an MSc degree in Computer Science from the University of Jordan, Amman, Jordan, in 2003, and his Ph.D. in Computer Science from the Faculty of Science and Technology at Anglia University, UK, in 2009. Currently, he is an Associate professor of computer science at Princess Sumaya University for Technology (PSUT). His research interests include computer security, cryptography, identification and authentication, wireless and mobile networks security, e-application security, machine learning, and other related topics. He can be contacted at email: m.alfayoumi@psut.edu.jo






Ammar Odeh    received his Ph.D. Degree in Computer science and Engineering with a concentration in Computer Security (Steganography) from University of Bridgeport. He received M.S. degree in Computer Science with a concentration in Reverse software Engineering and Computer Security from the University of Jordan, College of King Abdullah II School for Information Technology (KASIT). In 2002, he finished B.Sc. Degree in Computer Science and applications, from the Hashemite University, Prince Al-Hussein Bin Abdullah II for Information Technology. During the Ph.D. period, he worked as research Assistant, Teaching Assistant, and Instructor. He is currently an assistant professor in the computer science at Princess Sumaya University for Technology. He can be contacted at email: a.odeh@psut.edu.jo.



Ismail Keshta    received his B.Sc. and the M.Sc. degrees in computer engineering and his Ph.D. in computer science and engineering from the King Fahd University of Petroleum and Minerals (KFUPM), Dhahran, Saudi Arabia, in 2009, 2011, and 2016, respectively. He was a lecturer in the Computer Engineering Department of KFUPM from 2012 to 2016. Prior to that, in 2011, he was a lecturer in Princess Nourah bint Abdulrahman University and Imam Muhammad ibn Saud Islamic University, Riyadh, Saudi Arabia. He is currently an assistant professor in the computer science and information systems department of AlMaarefa University, Riyadh, Saudi Arabia. His research interests include software process improvement, modeling, and intelligent systems. He can be contacted at email: imohamed@mcst.edu.sa.



Dr. Ashraf Ahmad    is currently an Associate Professor at Princess Sumya University for Technology (PSUT). Having obtained his B.Sc. from PSUT, Dr. Ahmad went on to obtain his PhD degree in Computer Science and Engineering from National Chiao Tung University (NCTU) in Taiwan, graduating with distinction. He can be contacted at email: a.ahmad@psut.edu.jo.