

Medical image encryption techniques: a technical survey and potential challenges

Ammar Odeh, Qasem Abu Al-Haija

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

Article Info

Article history:

Received Apr 19, 2022

Revised Sep 6, 2022

Accepted Oct 1, 2022

Keywords:

Confidentiality, integrity, and availability

Entropy

Health care

Telemedicine

Watermarking

ABSTRACT

Among the most sensitive and important data in telemedicine systems are medical images. It is necessary to use a robust encryption method that is resistant to cryptographic assaults while transferring medical images over the internet. Confidentiality is the most crucial of the three security goals for protecting information systems, along with availability, integrity, and compliance. Encryption and watermarking of medical images address problems with confidentiality and integrity in telemedicine applications. The need to prioritize security issues in telemedicine applications makes the choice of a trustworthy and efficient strategy or framework all the more crucial. The paper examines various security issues and cutting-edge methods to secure medical images for use with telemedicine systems.

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

Khalil Al-Saket St, Amman, Jordan

Email: a.odeh@psut.edu.jo

1. INTRODUCTION

Numerous techniques are used in medical diagnosis, such as ultrasonography, magnetic resonance imaging, and positron emission tomography. Diagnostic images undergo a wide range of operations, including feature selection, image denoising, and segmentation, and they are massively stored and shared [1]. Additionally, medical photographs, many of which contain confidential patient confidential details, are frequently transmitted via hospital intranets and the internet. The internet has serious problems like harmful tampering and data leakage, and hospital intranets lack reliable security solutions [2], [3].

A growing amount of multimedia data is being conveyed across unsecured communication channels as a result of the quick development of communications networks. User data security is essential for protecting users from harmful attacks, preventing data loss, and assuring data integrity because user data frequently contains private and confidential information. Currently, a variety of techniques, including digital watermarking, and encryption, can offer medical images a high level of security [4], [5].

Telemedicine uses information and communications networks to deliver clinical treatment to patients located far away. This has been utilized to overcome distance and access limitations in rural locations lacking clinical center services [6]. In urgent emergencies, it is also utilized to save lives. Telehealth is becoming increasingly popular for producing, transmitting, and storing enormous amounts of electronic patient information and medical reports [7]. Different telehealth platforms and models are also evolving, and how clinical health data is accessed and used is changing. Medical picture encryption addresses the confidentiality difficulties that arise in telemedicine applications. Intervention and illegal use of medical data can be avoided when the medical image pixels are jumbled and encrypted using numerous ways [8].

An image that can be recognized can be made unrecognizable using encryption techniques. One of the easiest ways to defend the confidentiality of patients' personal information on public networks from hostile attacks is by the use of medical picture encryption, such as that used for mammograms, magnetic resonance imaging (MRIs), chest X-rays, computerized tomography (CT) scans, and other similar images. Medical applications in real-world settings face a serious issue in ensuring medical pictures' secure storage and transfer since they contain sensitive information about patients [9], [10].

One of the most popular uses of cryptographic protocols is to encrypt medical images, and this should be done using methods that are less expensive and time-consuming. When encrypting an image, symmetric or asymmetric encryption methods must be used to convert the input image into a cipher image using symmetric or asymmetric keys. While symmetric ciphers utilize the same key for both encryption and decryption, asymmetric ciphers employ separate keys [3], [8].

The encryption of medical images can be done using a variety of methods and parameters. Medical picture encryption techniques include high-speed scrambling [2], bitwise XOR diffusion, chaos and edge maps, among others. The effectiveness of the algorithm for encrypting medical images can be assessed using metrics such as peak signal-to-noise ratio (PSNR), bit error rate, fidelity, and mean square error [2], [3]. to give a general review of the problems with medical image security. How to guarantee medical image availability, confidentiality, and integrity. The current essay aims to accomplish the following clear goals: i) to identify confidentiality, integrity, and availability; ii) to describe the methods used for medical image encryption; iii) to describe the evaluation metrics for medical image encryption techniques.

2. SECURITY PRINCIPLES

The security of an organization's systems is a top concern in the modern world. The main objective of any organization is to protect its data from hackers. In cryptography, there are two types of attacks: passive attacks and active attacks [11]. While passive attacks just obtain information from the system without having any impact on it, active assaults extract information from the system while altering its resources and operations [12]. Figure 1 illustrates how to test the information security triangle of privacy, consistency, and identification to shield data from attackers.

- Confidentiality: the degree of confidentiality determines how secret the information is. Only the sender and the receiver will have control over the information transferred between them, according to the principle. The confidentiality of the message is compromised if a service provider has access [13].
- Integrity: integrity makes sure that the information received is accurate and precise when the material of a message is changed after it has been transmitted. Even yet, it is asserted that the integrity of the communication has already been damaged before it reaches the destination recipient [14].
- Availability: the availability principle states that the authorized party will always have access to the resources. Information will not be used if it is not easily accessible. The information available should be sufficient to meet the user's needs.

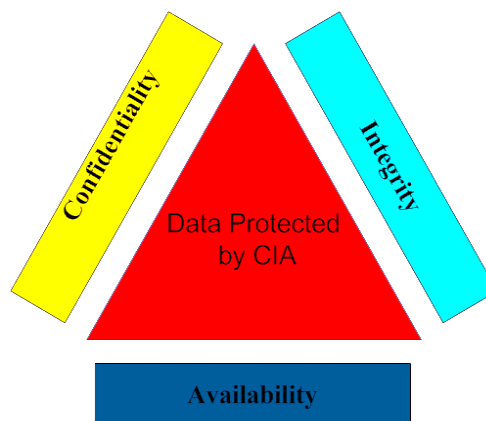


Figure 1. Confidentiality, integrity, and availability (CIA triad)

Both the business and its clients suffer when technologies, applications, and information are not available when authorized users need them. This term ties the state of networks, services, and programs to availability. It guarantees that when resources are required, legitimate people will have prompt, dependable

access to them [15]. Availability could be threatened by a wide range of factors, including hardware or software failure, power outages, natural disasters, and human error. The most well-known attack that endangers availability is undoubtedly the denial-of-service attack, in which a system, website, online application, or web-based service has its performance purposefully and maliciously degraded or is completely unavailable [16]. A few of the countermeasures that can assist ensure availability are duplication, hardware failures tolerance, systematic software patching and system upgrades, backups, thorough recovery plans, and denial-of-service prevention solutions [17]. Figure 2 depicts the components of the encryption block, which encrypts medical images using a secret key to prevent unauthorized access during storage or transmission through a telemedicine system.

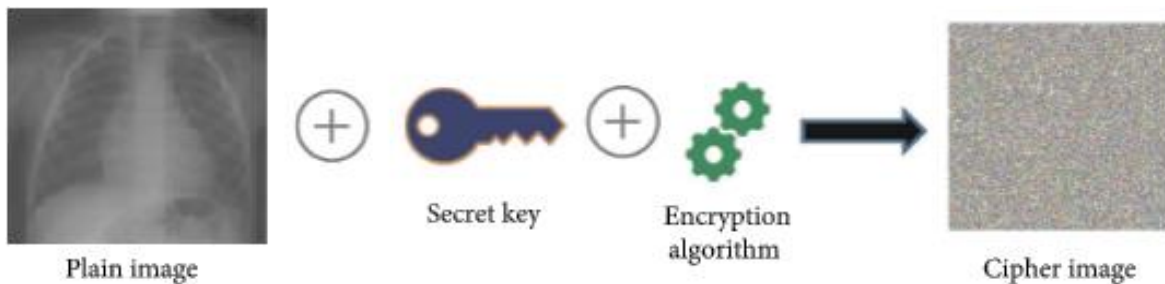


Figure 2. Encryption block for medical image

3. MEDICAL IMAGE ENCRYPTION TECHNIQUES

3.1. Edge maps for medical image encryption

Edge maps from a source image are used in a medical image encryption technique. Bit-plane decomposition, random sequence generator, and permutation are the three pieces that make up the algorithm. The following options are available to users: i) any image can be utilized as the source image, ii) various edge detectors and thresholds can generate different edge maps, iii) the selection of an appropriate bit-plane decomposition method is adjustable, and iv) the suggested algorithm can cascade several permutation methods. The suggested algorithm to protect various medical photographs has a significant keyspace and a high key sensitivity. Furthermore, it has broader applicability than other fuzzy edge map approaches [18].

3.2. Watermarking

Watermarking can increase the security of medical images by discretely adding specific information, also referred to as a watermark or secret data. In a binary format, the watermark data is usually added to the host image's pixel value. The information can then be recovered and utilized to establish the integrity of the medical image and its authenticity (belonging to the proper patient) [8]. Various watermarking techniques can be categorized based on how they are used. Based on the idea of embedding information, watermarking algorithms can be categorized as either spatial or transform domains. The host or cover image's pixel value in the spatial domain directly contains the watermark information. These techniques can insert a lot of watermarks and are quick and simple to apply. The key drawback of spatial domain techniques is their susceptibility to noise and lossy compression attacks, despite the fact that they have some advantages and can withstand cropping attacks. Furthermore, once a third party learns about the method, embedded watermarks can be updated. The watermark is embedded onto the original Image's modified version to produce the watermarked image in the transform domain. Watermarking techniques can be categorized as visible and invisible watermarks based on how people perceive them. For content or copyright protection, logos put at the corners of images or videos are a well-known example of visible approaches. Copyright protection, integrity verification, and authentication can all be accomplished with invisible watermarks. It is possible to use both visible and invisible watermarking at once. In this case, the invisible watermark can be used as a fallback for the visible one. Dual watermarking is the name of the strategy [19].

3.3. Adaptive medical image encryption

Adaptive medical image encryption (AMIE) is an intelligent healthcare internet of things (IoT) solution that uses a methodology to build an accurate cipher image from a basic medical image [20]. The technique consists of several vital components used throughout the procedure to produce the desired results. To generate random shuffle pixel placements and changes in pixel values, the high-speed scrambling and

diffusion process completed rounds simultaneously. Performing rounds with the AMIE process resulted in a high-security level in encrypted cipher medical images [20].

4. LITERATURE SURVEY

The current study systematically reviews secondary literature relevant to the research issue. A competent research study can access secondary data from a reliable source and use it. According to Ehsan *et al.* [21], a significant amount of data has been archived over time. As a result, it is practicable to do secondary research using existing data and information. According to Zing *et al.* [22], Examining and interpreting data obtained by another researcher for a different purpose is known as secondary data analysis. This approach is a useful research technique that is less expensive and requires less time to gather data in the field. This method was adopted for this research because it considers the time and resources of the researcher. In order to formulate and implement therapies, Keshta and Odeh [16] claim that secondary data is readily available, helps to better define the issue, and provides a complete view of the situation. The most recent research guarantees that the information used is reliable, current, and pertinent to the study.

4.1. Sampling procedure

A secondary literature collection procedure comprised picking secondary data that was accessible online and had some relevance to issues of medical image confidentiality, integrity, availability challenges, and concerns for telemedicine. Any article selected as a sample for this study has to be particular to telemedicine, addressing CIA triad problems, and especially inside smart health care centers. The study was chosen for examination only if it met the inclusion criteria already written for the other thesis studies and scholarly review articles [23].

The study was conducted to uncover specific security and privacy vulnerabilities linked with medical image data obtained from dependable sources or collected via random sampling, among other things. Because of the various advantages of randomization over other data gathering methods, such as nonrandomized sampling, which in the majority of cases always has some business, data collected through the random sample was given priority during the systematic review process [24], [25].

A comprehensive literature study was one of the most successful approaches for analyzing the general issues of security, privacy, and trust challenges, as well as medical image concerns for competent health care concurrent systems. Only the data sources that looked to meet the criteria for inclusion had their content generated after the abstracts and titles of all of the links that had been picked were examined. To aid in the analysis, a hard copy was printed. The content of all of these data sources was then scanned to determine that they were linked to medical images for telemedicine systems confidentiality, integrity, and availability difficulties and concerns [16], [23].

Additionally, all identified sources were subjected to additional scrutiny to confirm that they were highly appropriate for inclusion in the study. The crucial issues in the evaluation included whether the article or publication appropriately addressed the study's overall goal. The reliability of the information source was also checked to see if the arguments in the books and articles were relevant to the hazards posed by medical imaging and to what degree the security and privacy concerns could be resolved [14].

4.2. Data collection process

To uncover instances of CIA triad breaches in medical imaging (MI) within the healthcare system, a literature analysis was carried out. The acceptable secondary sources for this review were journal articles, books, and periodicals on MI issues, including reliability, availability issues, and concerns. The database of the university library was used to find books and other intellectual publications. Each article was written by entering pertinent keywords into databases on computers. Peer-reviewed literature was looked up in several databases, including Google Scholar, EBSCOhost, ERIC, and Academic OneFile.

Numerous keywords were used during the search. Searches were conducted using the terms "Medical image encryption", "CIA for medical image", and "Security over telemedicine". The articles and papers from the aforementioned search results were chosen because they discussed a strategy or a group of suggestions for handling MI problems and issues for healthcare systems. 4,514 documents, including formal research studies and reports from other health organizations, were found using a search strategy across multiple organization databases. The search method made a lot of data accessible, but all duplicates were eliminated through data cleaning.

After the duplicates were eliminated, the titles and abstracts of the remaining 2,581 articles were examined. Due to the fact that they did not meet the eligibility conditions, 1,850 persons were excluded. Additionally, there was no research on "ongoing review" present. Due to their methodology and design, other studies were excluded. Figure 3 of the PRISMA research flowchart shows the search results.

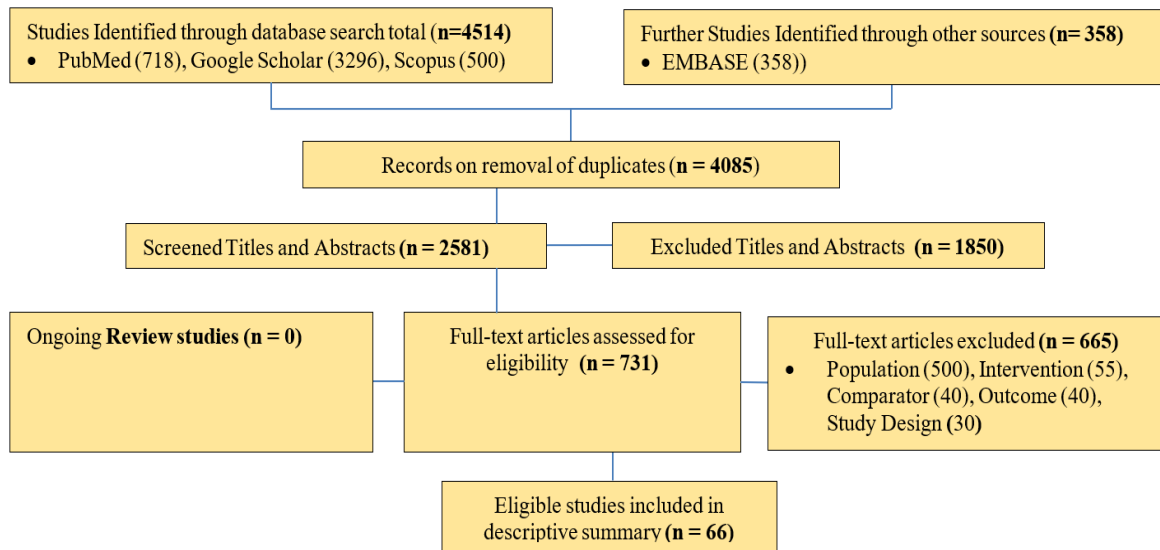


Figure 3. PRISMA study flowchart of search results

5. DISCUSSION OF FINDINGS AND DISCUSSION

A medical image encryption technique based on edge maps produced from a source image is presented in this research. The algorithm comprises three parts: bit-plane decomposition, random sequence generator, and permutation. The suggested technique for protecting various medical images has a considerable key space and a high key sensitivity. It also has broader applicability than other fuzzy edge map approaches [26].

The discrete wavelet transform (DWT) block-based scrambling technique proposed in this research is utilized for medical image encryption and uses edge maps generated from a source image. The approach is divided into three stages: DWT-plane decomposition, edge map sequence generation, and DWT-level scrambling. The proposed method yields a 99.592% number of pixel change rates and a 34.268% unified average hanged intensity. In addition, simulations and security analyses demonstrate strong resistance to various security assaults and outperform other traditional methods [27].

A method for encrypting medical images has been proposed that is both efficient and effective. The secret keys were retrieved using a six-dimensional hyperchaotic map. A standard medical image was separated into three channels: red, green, and blue. To diffuse these channels, secret keys were utilized. Finally, the encrypted channels were combined to create an encrypted medical image [28].

The suggested method has the advantages of requiring just one key image smaller than or equal to the original image's size, and RC4 encryption achieves intense visual scrambling with minimal temporal complexity. Furthermore, copyright protection is provided via watermarking, and incorporating patient information saves space. Furthermore, the proposed approach is impervious to key guessing attacks [29]. Improved Henon maps, integer wavelet transform (IWT), bit-plane decomposition, and deoxyribonucleic acid (DNA) sequence operations are combined to develop a hybrid domain picture encryption approach. And start with the usual two-dimensional Henon map [30].

The research provides an enhanced ElGamal encryption algorithm for medical image encryption. Separate calculations for encoding a plain message to an elliptic curve coordinate have been omitted from the proposed approach, which is a new finding. The updated version of the ElGamal encryption scheme's algorithm is meant to encrypt medical images, with data expansion issues handled and execution performance improved. Various statistical and security evaluations and comparisons with other encryption techniques ensure the strength of the suggested solution [31].

Kamali *et al.* [32] proposes a medical image encryption technique based on scrambling and confusion. The addresses of the medical picture pixels are scrambled using a chaotic cat map. A modified version of the simplified version of advance encryption standard (S-AES) is introduced and used to offer security for the scheme. The difference is that we utilize S-AES instead of chaos for S-box design. The so-called chaotic S-AES has all of S-AES' cryptographic properties and requirements. As a result, the work's essential contribution is the employment of chaos in the picture diffusion and confusion sections.

The usage of a chaotic map on the fractional discrete cosine transform (FrDCT) coefficients of the medical data/images is described in [33] as a new strategy for ensuring the safety of medical data. The

mandatory fractional discrete cosine transform (FrDCT) allows for great flexibility in the encryption of medical images. The algorithm consists of two major steps: applying FrDCT to an image and then applying a chaotic map to the FrDCT coefficients.

In [34], [35], the use of electrocardiogram (ECG) signals for the medical image encryption (ImgEnc) technique is proposed. It will use the generalized Arnold and chaotic logistic maps (Cat Map). The ECG signal and the wolf algorithm produce beginning conditions for chaotic maps (ChMp). Only the encryption procedure uses autoblocking diffusion (AutBlk). The primary stream is formed by a control parameter generated from the basic image (planning), effective and safe against plaintext (plaintext) and known plaintext attacks. According to experimental findings, the suggested algorithm may provide high security with good efficiency.

Studies [36], [37], offer a general-purpose method for encrypting medical images that is built on a novel union of dynamic substitution boxes (S-boxes) and chaotic maps, two extremely effective structures. S-box substitution successfully withstands selected plaintext and cipher text attacks when applied both before and after the chaotic substitution. Pseudorandom number generators are guarded against the reset attack with special measures. We demonstrate how to create the general framework using any chaotic map and any key-dependent dynamic S-box creation technique.

Selvi [38] combine elliptic curve cryptography with homomorphic encryption to provide better elliptic curve cryptography. Because traditional elliptic curve cryptography has several flaws, we begin by improving elliptic curve cryptography. Then, in medical picture encryption, modified elliptic curve cryptography is combined with homomorphic encryption. Compared to existing algorithms, the testing results demonstrate that this new method has a good encryption effect, high security, and many keys.

6. COMPARISON OF ENCRYPTION TECHNIQUES

Table 1 compares a distinguished set of algorithms provided for encoding medical images. The comparison was based on color space, encryption time, Entropy, and correlation coefficient. A collection of colors arranged in a certain way is known as a color space. When used in conjunction with color profiling made possible by various physical equipment, it helps create repeatable representations of color whether the model is an analog or digital image. The most basic color space is gray (called white). Gray space is a single dimension or component that runs from pure white to pure black and is used for grayscale printing. A red green blue (RGB) color space is produced by the transfer function, also known as the tone response curve, the white point, which is commonly a standard illuminant .The length of time required by an encryption procedure to transform plaintext into encrypted text is known as the encryption time. The throughput of an encryption method is calculated using the encryption time.

Table 1. Evaluation metrics

Ref	Color	Image Size	processing time(s)	Entropy	correlation coefficient
[30]	Gray	512*512	00.35	7.99	0.00136
[31]	Gray	512*513	2.382	7.9559	0.531
[33]	Gray	512*514	0.5	7.89	0.00116
[36]	Gray	512*515	5.9	7.9886	0.001197
[38]	Gray	512*516	1.33	7.88	0.00012
[28]	RGB	512*517	1.759	7.87	0.00133
[38]	Gray	257*256	2.35	7.93	0.0097
[39]	RGB	512*512	0.220	8.00	0.0071

7. CONCLUDING REMARKS

It is critical to protect medical data against forgeries and fraud in today's technological environment with high-speed communication. It is becoming more difficult to transfer large amounts of medical data as internet users grow. Because this (medical data) is frequently utilized for various diagnostic reasons, the information in medical photographs must be safeguarded. It is a legal responsibility to protect patient privacy and medical records. Traditional encryption approaches cannot deal with the vast volume of medical imaging data and its unique statistical features. A thorough review of the relevant literature serves as the foundation for this study's creation of a multidimensional taxonomy for medical image encryption. Edge maps, watermarking, and adaptive medical picture encryption are the three dimensions that make up the taxonomy's comprehensive view of medical image encryption. The research also closes a gap in the study of medical image encryption countermeasures through a methodical investigation. The suggested taxonomy also identifies security principal vectors including confidentiality, integrity, and availability to measure the effectiveness of the encryption model in protecting medical images. These findings point to a number of

unresolved problems for further study and improvement in medical picture encryption and prevention approaches, including patient information fabrication or unauthorized access, both of which have a negative impact on the diagnosis process. Beyond just identifying the problem, we offer potential remedies based on the proposed classification of countermeasures, as well as through the use of blockchain technology, machine learning, and deep learning methods.

ACKNOWLEDGMENT

This research was supported by Princess Sumaya University for Technology (PSUT).





REFERENCES

- [1] 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, Nov. 2021, doi: 10.1109/JSEN.2021.3114266.
- [2] 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, Apr. 2019, doi: 10.1016/j.jacr.2018.09.050.
- [3] 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, Jan. 2020, doi: 10.1016/j.comcom.2019.12.030.
- [4] S. Ben Atitallah, M. Driss, W. Boulila, and H. Ben Ghézala, "Leveraging deep learning and IoT big data analytics to support the smart cities development: review and future directions," *Computer Science Review*, vol. 38, Nov. 2020, doi: 10.1016/j.cosrev.2020.100303.
- [5] H. Ayesha *et al.*, "Automatic medical image interpretation: State of the art and future directions," *Pattern Recognition*, vol. 114, Jun. 2021, doi: 10.1016/j.patcog.2021.107856.
- [6] A. Banu S and R. Amirharajan, "A robust medical image encryption in dual domain: chaos-DNA-IWT combined approach," *Medical and Biological Engineering and Computing*, vol. 58, no. 7, pp. 1445–1458, Jul. 2020, doi: 10.1007/s11517-020-02178-w.
- [7] B. P. Battula and D. Balaganesh, "Medical image data classification using deep learning based hybrid model with CNN and encoder," *Revue d'Intelligence Artificielle*, vol. 34, no. 5, pp. 645–652, Nov. 2020, doi: 10.18280/ria.340516.
- [8] M. Begum and M. S. Uddin, "Digital image watermarking techniques: a review," *Information*, vol. 11, no. 2, Feb. 2020, doi: 10.3390/info11020110.
- [9] 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, Jun. 2020, doi: 10.21037/atm.2020.02.44.
- [10] Q. Duan *et al.*, "SenseCare: A research platform for medical image informatics and interactive 3D visualization," *arXiv preprint arXiv: 2004.07031*, Apr. 2020.
- [11] 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.
- [12] 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, Feb. 2020, doi: 10.1016/j.ijinfomgt.2019.05.003.
- [13] H. M. Ghadirli, A. Nodehi, and R. Enayatifar, "An overview of encryption algorithms in color images," *Signal Processing*, vol. 164, pp. 163–185, Nov. 2019, doi: 10.1016/j.sigpro.2019.06.010.
- [14] 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, no. S14, Dec. 2020, doi: 10.1186/s12911-020-01328-2.
- [15] 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, Aug. 2021, doi: 10.3390/app11178117.
- [16] I. Keshta and A. Odeh, "Security and privacy of electronic health records: Concerns and challenges," *Egyptian Informatics Journal*, vol. 22, no. 2, pp. 177–183, 2021, doi: 10.1016/j.eij.2020.07.003.
- [17] R. R. Paulsen and T. B. Moeslund, *Introduction to medical image analysis*. Cham: Springer International Publishing, 2020, doi: 10.1007/978-3-030-39364-9.
- [18] W. Cao, Y. Zhou, C. L. P. Chen, and L. Xia, "Medical image encryption using edge maps," *Signal Processing*, vol. 132, pp. 96–109, Mar. 2017, doi: 10.1016/j.sigpro.2016.10.003.
- [19] S. Haddad, G. Coatrieux, A. Moreau-Gaudry, and M. Cozic, "Joint Watermarking-Encryption-JPEG-LS for medical image reliability control in encrypted and compressed domains," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 2556–2569, 2020, doi: 10.1109/TIFS.2020.2972159.
- [20] X. Chai, J. Zhang, Z. Gan, and Y. Zhang, "Medical image encryption algorithm based on Latin square and memristive chaotic system," *Multimedia Tools and Applications*, vol. 78, no. 24, pp. 35419–35453, Dec. 2019, doi: 10.1007/s11042-019-08168-x.
- [21] A. Ehsan, H. S. Klaas, A. Bastianen, and D. Spini, "Social capital and health: A systematic review of systematic reviews," *SSM-Population Health*, vol. 8, Aug. 2019, doi: 10.1016/j.ssmph.2019.100425.
- [22] X. Zeng *et al.*, "The methodological quality assessment tools for preclinical and clinical studies, systematic review and meta-analysis, and clinical practice guideline: a systematic review," *Journal of Evidence-Based Medicine*, vol. 8, no. 1, pp. 2–10, Feb. 2015, doi: 10.1111/jebm.12141.
- [23] T. Poletto, M. M. Silva, T. R. N. Clemente, A. P. H. de Gusmão, A. P. de 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, Apr. 2021, doi: 10.3390/s21072426.
- [24] P. Savadjiev *et al.*, "Demystification of AI-driven medical image interpretation: past, present and future," *European Radiology*, vol. 29, no. 3, pp. 1616–1624, Mar. 2019, doi: 10.1007/s00330-018-5674-x.
- [25] R. Pratap 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, Jul. 2020, doi: 10.1016/j.jcot.2020.05.011.
- [26] J. Kasurinen and A. Knutas, "Publication trends in gamification: A systematic mapping study," *Computer Science Review*, vol. 27, pp. 33–44, Feb. 2018, doi: 10.1016/j.cosrev.2017.10.003.
- [27] A. B. Joshi, D. Kumar, D. C. Mishra, and V. Guleria, "Colour-image encryption based on 2D discrete wavelet transform and 3D logistic chaotic map," *Journal of Modern Optics*, vol. 67, no. 10, pp. 933–949, Jun. 2020, doi: 10.1080/09500340.2020.1789233.





- [28] Y. Tian and Z. Lu, "S-box: Six-dimensional compound hyperchaotic map and artificial bee colony algorithm," *Journal of Systems Engineering and Electronics*, vol. 27, no. 1, pp. 232–241, 2016.
- [29] I. B. Venkateswarlu, "Fast medical image security using color channel encryption," *Brazilian Archives of Biology and Technology*, vol. 63, 2020, doi: 10.1590/1678-4324-2020180473.
- [30] X. Zhang and X. Wang, "Multiple-image encryption algorithm based on mixed image element and chaos," *Computers and Electrical Engineering*, vol. 62, pp. 401–413, Aug. 2017, doi: 10.1016/j.compeleceng.2016.12.025.
- [31] D. S. Laiphrakpam and M. S. Khumanthem, "Medical image encryption based on improved ElGamal encryption technique," *Optik*, vol. 147, pp. 88–102, Oct. 2017, doi: 10.1016/j.ijleo.2017.08.028.
- [32] S. H. Kamali, R. Shakerian, M. Hedayati, and M. Rahmani, "A new modified version of advanced encryption standard based algorithm for image encryption," in *2010 International Conference on Electronics and Information Engineering*, Aug. 2010, pp. 141–145. doi: 10.1109/ICEIE.2010.5559902.
- [33] S. Kumar, B. Panna, and R. K. Jha, "Medical image encryption using fractional discrete cosine transform with chaotic function," *Medical and Biological Engineering and Computing*, vol. 57, no. 11, pp. 2517–2533, Nov. 2019, doi: 10.1007/s11517-019-02037-3.
- [34] A. S. Abdulbaqi, A. J. Obaid, and A. H. Mohammed, "ECG signals recruitment to implement a new technique for medical image encryption," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 24, no. 6, pp. 1663–1673, Aug. 2021, doi: 10.1080/09720529.2021.1884378.
- [35] A. Odeh, I. Keshta, and Q. A. Al-Haija, "Analysis of blockchain in the healthcare sector: application and issues," *Symmetry*, vol. 14, no. 9, Aug. 2022, doi: 10.3390/sym14091760.
- [36] I. Hussain, T. Shah, and M. Asif Gondal, "An efficient image encryption algorithm based on S8 S-box transformation and NCA map," *Optics Communications*, vol. 285, no. 24, pp. 4887–4890, Nov. 2012, doi: 10.1016/j.optcom.2012.06.011.
- [37] Q. A. Al-Haija, M. Gharaibeh, and A. Odeh, "Detection in adverse weather conditions for autonomous vehicles via deep learning," *AI*, vol. 3, no. 2, pp. 303–317, Apr. 2022, doi: 10.3390/ai3020019.
- [38] S. Selvi, "An efficient hybrid cryptography model for cloud data security," *International Journal of Computer Science and Information Security (IJCSIS)*, vol. 15, no. 5, 2017.
- [39] A. Ahmad, Y. AbuHour, R. Younis, Y. Alslman, E. Alnagi, and Q. Abu Al-Haija, "MID-Crypt: a cryptographic algorithm for advanced medical images protection," *Journal of Sensor and Actuator Networks*, vol. 11, no. 2, May 2022, doi: 10.3390/jsan11020024.

BIOGRAPHIES OF AUTHORS



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



Qasem Abu Al-Haija     received his Ph.D. from Tennessee State University (TSU), the USA, in 2020. He is currently an Assistant Professor at the Department of Computer Science/Cybersecurity, School of Computing Sciences, Princess Sumaya University for Technology (PSUT), Amman, Jordan. He is the author of more than 100 scientific research papers and book chapters. His research interests include AI, Cybersecurity, IoT, CPS, cryptography, and networks. He can be contacted at email: q.abualhaija@psut.edu.jo.