A New JPEG Compression Algorithm for Transmission, Processing and Storage of Health Data

Yılmaz Aydın
Department of Software Engineering
Fırat University
Elazig, Turkey
y.aydin@firat.edu.tr

Fatih Özkaynak
Department of Software Engineering
Fırat University
Elazig, Turkey
ozkaynak@firat.edu.tr

***Abstract*—This study proposes a new compression algorithm for health data management, which is a derivative of the JPEG algorithm. The proposed method has shown improvement in compression ratio compared to the classical JPEG algorithm, making it a promising solution for the storage and transmission of medical images in PACS systems. The algorithm has been designed with data security in mind and it is planned to integrate it with encryption algorithms in the future. The performance of the proposed algorithm was evaluated through comprehensive testing, and its potential real-world applications were discussed. The results of this study demonstrate the feasibility of the proposed algorithm and suggest that it has the potential to revolutionize the field of health data management. This study provides a roadmap for future work on the proposed algorithm, including its integration with encryption algorithms, performance evaluations, real-world implementation, and continuous improvement**

Keywords—Data compression, DICOM, PACS, JPEG

I. Introduction

Medical imaging plays a crucial role in healthcare, and the efficient storage and transmission of these images is critical for delivering effective patient care. The DICOM standard is widely used for storing and transmitting medical images, and the JPEG algorithm is one of the primary methods for compressing these images in DICOM. However, with the increasing volume of medical data being generated, there is a growing need for more efficient data compression algorithms [1, 2].

Data management systems aims to reducing the amount of storage space required for data, as well as the amount of bandwidth required for data transmission [3]. Data compression techniques help to reduce the cost of storage and improve the speed and efficiency of data transfer. Additionally, data compression can also enhance the security of data by reducing the amount of sensitive information that needs to be transmitted, which minimizes the risk of unauthorized access.

In this article, we present a new compression algorithm for health data management that improves upon the classical JPEG algorithm. Our approach is a derivative of a new JPEG algorithm and is specifically designed to address the challenges of compressing medical images. By combining the strengths of both JPEG and our new approach, we are able to achieve a significant improvement in the compression ratio compared to the classical JPEG algorithm [4].

The rest of the article can then go on to describe the method in more detail, present the results of experiments comparing the new algorithm to classical JPEG, and discuss the implications of the results for health data management.

II. Data Management in Health Sector

Data management encompasses the entire process from data collection, storage, protection, analysis and sharing. Data management is important to ensure the accuracy, security and accessibility of data. Also, data needs to be processed and analyzed to make it meaningful and useful [5-7]. For this, data management teams must address issues such as data quality, data storage, data access, and data security. Data management is also important to ensure that data is used in accordance with legal and ethical rules. Today, developments such as big data and cloud computing show that data management has become even more important. There are many different ways to manage data, ensure the accuracy, security and accessibility of data.

Data quality: Data management teams should perform data quality control to ensure the accuracy and reliability of the data. These processes include data entry control, data cleaning, data validation, and data standardization.

Data storage: Data storage management is important for the secure storage and protection of data. These operations include data backup, data archiving and data restoration.

Data access: Data access management is important so that data is easily accessible to those who need it. These processes include data cataloging, data access control, and data access monitoring.

Data security: Data security management is important to ensure data security. These processes include data encryption, data security policies, data security training.

Legal and Ethical Rules: To ensure that data is used in accordance with legal and ethical rules, data management teams must follow data legal obligations and ethical rules.

In order to run a successful data management process, all these listed steps need to be considered as a whole. Because;

there are several threats that can arise when processing, transmitting, and storing health data, including [8-10]:

- Cyber-attacks: Health data is a valuable target for cybercriminals, who can use various techniques to gain unauthorized access to the data, such as phishing, malware, and ransomware.
- Insider threats: Employees or contractors with access to health data can misuse or steal the data, either intentionally or unintentionally.
- Social engineering: Criminals can use social engineering techniques, such as phishing, to trick individuals into revealing sensitive information or providing access to systems.
- Physical threats: Health data can be compromised by physical threats, such as theft of devices, natural disasters, or power outages.
- Data breaches: Health data can be compromised as a result of data breaches, which can occur due to a variety of factors, such as software vulnerabilities, weak passwords, or lack of security controls.
- Compliance issues: Organizations may fail to comply with laws and regulations related to the protection of personal health information, which can lead to penalties and reputational damage.
- Privacy concerns: Health data can be used for unauthorized purposes, such as targeted advertising or discrimination.
- Interoperability challenges: As health data is shared between different systems and organizations, challenges can arise in ensuring that the data is accurate and accessible to authorized individuals.
- Misuse of data: Health data can be used for unauthorized purposes, such as research or marketing activities without the proper consent of the individuals.

It's important to note that these are not the only potential threats and new ones may emerge as technology and data sharing practices evolve. For example; there are several sources that report statistics on the frequency of stolen patient data, but the numbers can vary depending on the source and the definition of "stolen" data. According to the Protenus Breach Barometer, in 2020, there were over 500 breaches of patient data reported, affecting over 20 million individuals. The healthcare sector accounted for the second-highest number of breaches of any industry. The Identity Theft Resource Center reported that healthcare data breaches accounted for 32.7% of all data breaches in 2020. Ponemon Institute's 2020 Cost of a Data Breach Report states that the average cost of a data breach in the healthcare industry is $7.13 million. However, it's important to note that these numbers are just the reported cases and it is quite possible that many cases go unreported. It's worth noting that these numbers are not only for stolen patient data but for all kind of breaches that includes lost laptops, stolen devices, and employee error [11].

The problem is so serious that the issue of unauthorized access to personal health information is a concern globally. Different countries have different laws and regulations in place to protect personal health information, and the enforcement of these laws can vary. For example, in the United States, the Health Insurance Portability and Accountability Act (HIPAA) [12] sets national standards for protecting personal health information. The Office for Civil Rights (OCR) within the Department of Health and Human Services (HHS) is responsible for enforcing these standards. In the European Union, the General Data Protection Regulation (GDPR) [13] provides a comprehensive framework for protecting personal data, including personal health information. The GDPR applies to all organizations operating within the EU, as well as organizations outside of the EU that process personal data about EU citizens. In Canada, the Personal Information Protection and Electronic Documents Act (PIPEDA) sets the rules for the collection, use, and disclosure of personal information in the private sector. In Australia, the Privacy Act 1988 regulates the handling of personal information, including health information. The Office of the Australian Information Commissioner (OAIC) is responsible for enforcing the Privacy Act. Most countries have laws and regulations in place to protect personal health information, but the level of enforcement and the penalties for non-compliance can vary. Additionally, the issue of unauthorized access to personal health information is not limited to any specific region or country, and it is a global concern.

How to improve the management of health data with artificial intelligence technologies has recently become an increasingly popular research area [14, 15]. The management of health data is vital for making health services efficient and effective. However, due to the size and complexity of health data, artificial intelligence technologies are gaining more and more importance in order to process this data and extract meaningful information. Artificial intelligence can be used as an important tool to extract meaningful information from health data [16, 17]. For example, AI algorithms can more accurately determine disease diagnoses and treatment options from health data. In addition, artificial intelligence can contribute to the improvement of personal health services by creating personal health profiles from health data. However, with the use of artificial intelligence technologies, the privacy and security of health data becomes more important. Therefore, when using artificial intelligence in the management of health data, data privacy and security issues need to be carefully considered.

A. Electronic Health Record System

An Electronic Health Record (EHR) system is a digital version of a patient's paper chart that is used to store and manage patient health information [18]. EHR systems are used by healthcare providers to manage patient information and improve the quality, safety, and efficiency of care. Many research companies regularly publish reports on the EHR market, which include data on the size and growth of the market, as well as information on the leading vendors and their market share. Gartner's "Magic Quadrant for EHR" report, evaluates and positions the EHR vendors based on their ability to execute and their completeness of vision. The report assesses the strengths and challenges of the EHR vendors, and provides a snapshot of the EHR market. The EHR market is a highly competitive one with a significant number of players. Gartner's report highlights the major EHR vendors [19], including Cerner, Epic Systems, Allscripts, athenahealth, and NextGen, as well as other well-known vendors such as Meditech, McKesson, and eClinicalWorks. According to Gartner's report, Cerner and Epic Systems are considered the leading EHR vendors, with Cerner being recognized as the leader in the EHR market with the highest market share, followed by Epic Systems. Other research firms such as KLAS Research, Black Book Research, and M Research also regularly publish reports on the EHR market, providing similar data and analysis on the EHR market and the leading vendors.

The EHR market size is a constantly evolving and growing. According to a report by MarketsandMarkets, the global EHR market size is expected to reach $41.5 billion by 2023 from $22.9 billion in 2018, at a CAGR of 11.9% during the forecast period. This is due to the increasing demand for EHR systems in the healthcare industry, due to the growing need for quality care, and the need to reduce healthcare costs. The North American region is expected to dominate the EHR market due to the presence of a large number of EHR vendors and the increasing adoption of EHR systems by healthcare providers in the region. The Asia Pacific region is expected to grow at the highest CAGR during the forecast period, due to the increasing government support for the adoption of EHR systems, the growing aging population, and the increasing prevalence of chronic diseases. According to a study by the Turkish Ministry of Health, the number of EHR systems in use by public hospitals in Turkey increased from 10% in 2010 to around 50% in 2016. The Turkish government has also been investing in the development of EHR systems and promoting their use in the healthcare sector as a way to improve the quality and efficiency of care. In Turkey, the Ministry of Health has been working on a centralized EHR system for the whole country. The system will allow for the sharing of patient data across different hospitals, and it's expected to improve the quality and safety of care, as well as reduce the risk of medical errors. Advantages of EHR systems include [20]:

- Improved patient care: EHR systems can provide healthcare providers with immediate access to patient information, including medical history, medications, and test results, which can improve the quality and safety of care.
- Increased efficiency: EHR systems can automate many of the tasks involved in managing patient information, such as scheduling appointments, ordering tests, and prescribing medications, which can save time and reduce errors.
- Better coordination of care: EHR systems can enable healthcare providers to share patient information with other providers and organizations, which can improve the coordination of care and reduce the risk of medical errors.
- Cost savings: EHR systems can reduce the need for paper records, which can save money and reduce administrative burdens.
- Improved population health management: EHR systems can provide healthcare providers with tools to identify patterns and trends in patient data, which can be used to improve the health of populations.

There are also some challenges and drawbacks associated with EHR systems, such as [21]:

- High costs: Implementing and maintaining EHR systems can be expensive, and may be a significant financial burden for healthcare providers.
- Interoperability issues: EHR systems from different vendors may not be able to share data easily, which can make it difficult for healthcare providers to access and use patient information from multiple sources.
- Privacy and security concerns: EHR systems store sensitive patient information, which can make them a target for cyberattacks. Ensuring the security and privacy of patient information is crucial and requires frequent updates and maintenance.
- User resistance: Some healthcare providers may be resistant to using EHR systems, which can make it difficult to fully realize the benefits of the technology.
- Data Quality and accuracy: Data entry errors are common, and if not corrected may lead to inaccurate patient information and potential adverse events.

Overall, EHR systems have the potential to greatly improve the quality, safety, and efficiency of healthcare. However, the successful implementation and use of EHR systems requires careful planning, investment, and ongoing maintenance to ensure that the benefits of the technology are fully realized. The development of EHR systems has progressed through several key milestones over the years:

1960s - The first EHR systems were developed in the 1960s, primarily as a way to automate the storage and retrieval of patient information. These early systems were primarily used in large teaching hospitals and research centers.

1980s - The 1980s saw the development of more advanced EHR systems, which began to include computerized decision support and clinical guidelines.

1990s - The 1990s saw the widespread adoption of EHR systems in hospitals and clinics, as well as the development of standards for the interoperability of EHR systems.

Early 2000s - The early 2000s saw the development of web-based EHR systems, which allowed for remote access to patient information and improved collaboration between healthcare providers.

Mid-2000s - The mid-2000s saw the introduction of Meaningful Use, a program established by the U.S. government to encourage the adoption of EHR systems and the use of the systems to improve patient care.

Late 2000s - The late 2000s saw the introduction of Personal Health Record (PHR) systems, which allowed patients to access and manage their own health information.

2010-2020 - The 2010-2020 decade marked the adoption and implementation of EHR systems across many countries and organizations. The development of cloud-based EHR systems and the increased focus on patient engagement also took place during this period.

2020-current - The current trend is towards more advanced EHR systems that leverage artificial intelligence, natural language processing, and machine learning to improve the efficiency and effectiveness of healthcare. Telemedicine and virtual care are also growing trends, with EHRs being used to support these new models of care.

III. Security Issues in EHR System

Data security aims to ensure that access to data is made only by authorized persons, that the use of data is in accordance with laws and rules, and that data is stored securely. Some basic steps that can be done to ensure data security are listed below [22, 23].

- Password and authentication: Access to data should only be done by authorized persons. Therefore, security measures such as password and authentication should be used.
- Data encryption: When data is stored encrypted, it is easier to prevent unauthorized access. Data encryption can be used to increase the security of data.
- Up-to-date security software: Security software can be used to secure data access and use. For example, software such as antivirus software or firewall can be used.
- Backup and restore: Backing up data ensure that data is protected from loss. In addition, restore operations allow data to be recovered and restored.
- Ethical rules: Data security also includes the use of data in accordance with the law and ethical rules. Therefore, ethical rules and regulations should be determined and implemented for data security.
- Training and Sensitivity: It is important that employees are educated and conscious about data security. For this reason, training and sensitization (sensitization, increasing sensitivity) programs on data security should be carried out and employees should be made aware of data security.
- Continuous updating and auditing: Continuous updating and auditing should be done on data security. For this reason, continuous audits and updates should be made on data security.

In fact, the issue of data security is a very broad field and includes many factors. Especially with constantly updated technologies and attack methods, continuous audits and updates are required. Within the scope of this study, the focus is on key generators in the field of data encryption. The rest of the study is organized as follows. In the second section, data management and security problems in the health sector are discussed. In the third section, the details of the encryption approach that can be used to ensure the security of electronic health data are given. In the last section, the results obtained are discussed and projections for future studies are presented

The extent of illegal access to health data is not widely available. However, it is a growing concern as more and more personal health information is being stored and shared electronically. The unauthorized access and use of personal health information can have serious consequences for individuals, including identity theft, financial fraud, and damage to one's reputation. Additionally, it can also compromise the security of the healthcare system as a whole, leading to a lack of trust in the system and reluctance to share sensitive information. There are several key elements to be considered in the process of processing, transmitting, and storing health data, including:

- **Confidentiality:** Health data is sensitive information that should be kept confidential and only shared with authorized individuals.
- **Integrity:** Health data should be accurate, complete, and protected from unauthorized alteration or destruction.
- **Availability:** Health data should be accessible to authorized individuals when needed.
- **Privacy:** Health data should be protected from unauthorized access and use.
- **Security:** Health data should be protected from unauthorized access, use, disclosure, disruption, modification, or destruction.
- **Compliance:** Health data should be processed and stored in compliance with relevant laws and regulations, such as the Health Insurance Portability and Accountability Act (HIPAA) in the United States and the General Data Protection Regulation (GDPR) in the European Union.
- **Encryption:** Health data should be encrypted while in transit and at rest to protect it from unauthorized access.
- **Backup and recovery:** Health data should be backed up regularly and a plan should be in place for recovery in case of a disaster or system failure. **Access controls:** Health data should be protected by strict access controls, including authentication and authorization, to ensure that only authorized individuals can access the data.
- **Auditing and monitoring:** Health data should be audited and monitored to detect and prevent unauthorized access or use. It's worth noting that these are general guidelines and specific regulations and laws might vary depending on the country, region or organization.

IV. Proposed Model

In the compression algorithm that is aimed to be developed, discrete fractional cosine transform is used instead of classical discrete cosine transform. Thanks to this modification, compression performance will be improved. The general view of the proposed model is given in Figure 1.

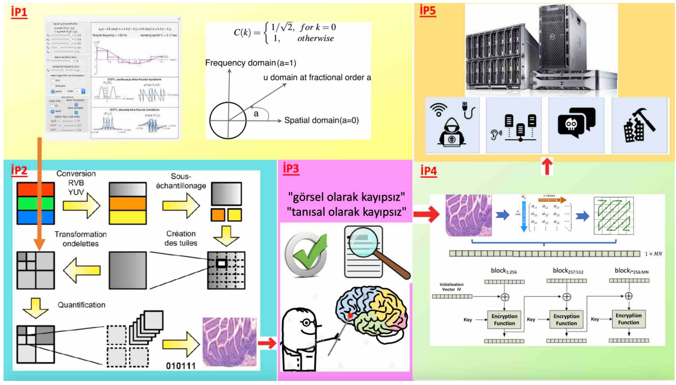

Fig. 1. The general view of proposed model

Figure 1 represents the use of a fractional discrete cosine transform instead of the classical discrete cosine transform in the yellow block. The proposed theoretical architecture aims to obtain new conversion tables by changing the fraction order, in other words, to improve the compression performance. Figure 1 blue block shows the JPEG algorithm step. It points out that the only difference of the approach proposed at this stage from the classical JPEG algorithm is the modification of the discrete cosine transform. The pink block indicates the integration of the process into PACS systems. The orange block draws attention to the security risks described in the study. The green block represents the encryption process that can be used to address security problems. In order to explain the operation of the method in a more detailed way, an example test image is given in Figure 2.

$$Orijinal = \begin{bmatrix} 154 & 123 & 123 & 123 & 123 & 123 & 123 & 136 \\ 192 & 180 & 136 & 154 & 154 & 154 & 136 & 110 \\ 254 & 198 & 154 & 154 & 180 & 154 & 123 & 123 \\ 239 & 180 & 136 & 180 & 180 & 166 & 123 & 123 \\ 180 & 154 & 136 & 167 & 166 & 149 & 136 & 136 \\ 128 & 136 & 123 & 136 & 154 & 180 & 198 & 154 \\ 123 & 105 & 110 & 149 & 136 & 136 & 180 & 166 \\ 110 & 136 & 123 & 123 & 123 & 136 & 154 & 136 \end{bmatrix}$$

Fig. 2. A sample test image

Let's say the sample test image is 8x8 in size. Each pixel color value corresponds to an integer value between 0-255. The intermediate value to be obtained in case of using the classical discrete cosine transform is shown in Figure 3.a. The value shown in the Figure 3.a is the last step of the JPEG algorithm, before the Huffman entropy coding. After this step, the image in the form of a two-dimensional matrix is read in a zig-zag form and converted into a one-dimensional array [24-27]. Then the array is compressed by entropy coding. In other words, the more 0s at the end of the array, the better the compression will be.

The hypothesis of the proposed study revolves around the potential positive impact of fractional-order transformations on the compression performance of the JPEG algorithm. To validate this hypothesis, emphasis has been placed on the discrete cosine step within the JPEG algorithm [28]. The primary novelty of the study lies in the acquisition of fractional-order transformations at 0.8 degrees within this article, instead of discrete cosine transformation. In the classical cosine transform, a zero value of 38 digits from the end is obtained. Intermediate values calculated when using alpha=0.8-degree discrete fractional cosine transform instead of classical discrete cosine transform are given in Figure 3.b. As a result of the calculations, if the image is converted to a one-dimensional array, it can be observed that the last 39 values are zero. With the proposed approach, it is possible to increase the compression performance of a small 8x8 image. he preliminary results obtained have indicated the significance of the proposed research question. Given the infinite number of fractional-order transformations within the [0,1] range, determining the most suitable transformation will be a crucial aspect for future studies.

$$C = \begin{bmatrix} 10 & 4 & 2 & 5 & 1 & 0 & 0 & 0 \\ 3 & 9 & 1 & 2 & 1 & 0 & 0 & 0 \\ -7 & -5 & 1 & -2 & -1 & 0 & 0 & 0 \\ -3 & -5 & 0 & -1 & 0 & 0 & 0 & 0 \\ -2 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \qquad C = \begin{bmatrix} 8 & 2 & 0 & 4 & 0 & 0 & 0 & 0 \\ 6 & 9 & 2 & 2 & 2 & 0 & 0 & 0 \\ -7 & -3 & 2 & -1 & 0 & 0 & 0 & 0 \\ -3 & -4 & 0 & -1 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 \\ 3 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix},$$

(a) (b)

Fig. 3. (a) result for classical-degree discrete fractional cosine transform (b) result for alpha=0.8-degree discrete fractional cosine transform

V. Conclusions

In conclusion, the new compression algorithm for health data management that we have developed has shown promising results. This method, which is a derivative of the widely used JPEG algorithm, has improved the compression ratio and is expected to play a significant role in optimizing the storage and transmission of medical images in PACS systems. The proposed approach has the potential to revolutionize the field of health data management by providing a more efficient and cost-effective solution for the storage and retrieval of medical images. We hope that our contribution will inspire further research and development in this area and lead to better outcomes for patients and the healthcare industry. Roadmap for future work on your compression and encryption algorithm for health data management:

- Integration with encryption algorithms: The first step in the roadmap would be to integrate the proposed compression algorithm with encryption algorithms such as AES or RSA to ensure the security of the medical images being stored and transmitted.

- Performance evaluation: The next step would be to conduct comprehensive performance evaluations of the combined compression and encryption algorithm. This will include measurements of compression ratio, encryption strength, and speed of data processing.

- Real-world implementation: The final step would be to implement the combined algorithm in real-world scenarios, such as hospital PACS systems, to assess its practicality and effectiveness in real-world scenarios.

- Continuous improvement: As with any new technology, it is important to continually assess and improve the proposed algorithm. This may include the incorporation of new encryption algorithms, the optimization of the compression method, and the integration of machine learning techniques to improve the efficiency of the algorithm.

This roadmap provides a clear path for future work on the proposed compression and encryption algorithm for health data management. By following these steps, we can ensure that the proposed solution provides maximum security and efficiency for the storage and transmission of medical images.

Acknowledgment

This paper was supported in part by the Scientific and Technological Research Council of Turkey (TÜBİTAK) under Grant 122R060.

References

[1] V. Suresh and S. Rajashree, "Establishing Authenticity for DICOM images using ECC algorithm," 2020 Sixth International Conference on Bio Signals, Images, and Instrumentation (ICBSII), Chennai, India, 2020, pp. 1-4, doi: 10.1109/ICBSII49132.2020.9167578.

[2] K. Belgacem, M. Kenoui, F. Bouguerra, M. Laidi, A. Semrani and C. Sellah, "Collaborative Visualization and Annotations of DICOM Images for Real-Time Web-based Telemedicine System," 2021 International Conference on Recent Advances in Mathematics and Informatics (ICRAMI), Tebessa, Algeria, 2021, pp. 1-6, doi: 10.1109/ICRAMI52622.2021.9585938.

[3] K. Hossain and S. Roy, "A Data Compression and Storage Optimization Framework for IoT Sensor Data in Cloud Storage," 2018 21st International Conference of Computer and Information Technology (ICCIT), Dhaka, Bangladesh, 2018, pp. 1-6, doi: 10.1109/ICCITECHN.2018.8631929.

[4] G. Hudson, A. Léger, B. Niss and I. Sebestyén, "JPEG at 25: Still Going Strong," in IEEE MultiMedia, vol. 24, no. 2, pp. 96-103, Apr.-June 2017, doi: 10.1109/MMUL.2017.38.

[5] S. Thakur, B. Gupta, U. Mathur and D. Bansal, "Electronic Health Record Systems for Enhanced Medical Care: A Survey," 2023 International Conference on Intelligent Systems for Communication, IoT and Security (ICISCoIS), Coimbatore, India, 2023, pp. 257-262, doi: 10.1109/ICISCoIS56541.2023.10100356.

[6] L. Mucaraku and M. Ali, "Importance of Information Systems in the Healthcare Sector," 2022 International Conference on Computing, Electronics & Communications Engineering (iCCECE), Southend, United Kingdom, 2022, pp. 112-117, doi: 10.1109/iCCECE55162.2022.9875083.

[7] H. Kaschel and A. Diaz, "High Security Ubiquitous H-IoT on a WBAN-based EHR using Blockchain," 2021 IEEE International Conference on Automation/XXIV Congress of the Chilean Association of Automatic Control (ICA-ACCA), Valparaíso, Chile, 2021, pp. 1-6, doi: 10.1109/ICAACCA51523.2021.9465266.

[8] M. Bakkar and A. Alazab, "Information Security: Definitions, Threats and Management in Dubai Hospitals Context," 2019 Cybersecurity and Cyberforensics Conference (CCC), Melbourne, VIC, Australia, 2019, pp. 152-159, doi: 10.1109/CCC.2019.00010.

[9] A. Y. Zalozhnev, D. A. Andros, V. N. Ginz and A. E. Loktionov, "Information Systems and Network Technologies for Personal Data Cyber Security in Public Health," 2019 International Multidisciplinary Information Technology and Engineering Conference (IMITEC), Vanderbijlpark, South Africa, 2019, pp. 1-5, doi: 10.1109/IMITEC45504.2019.9015844.

[10] J. Zhu and Z. Chen, "Exploration of Application Security for Medical Electronic Health Card," 2022 International Conference on Artificial Intelligence in Everything (AIE), Lefkosa, Cyprus, 2022, pp. 451-454, doi: 10.1109/AIE57029.2022.00092. https://blog.protenus.com/key-takeaways-from-the-2022-breach-barometer

[11] K. J. Nahra, "HIPAA Security Enforcement Is Here," in IEEE Security & Privacy, vol. 6, no. 6, pp. 70-72, Nov.-Dec. 2008, doi: 10.1109/MSP.2008.143.

[12] O. Amaral, S. Abualhaija, M. Sabetzadeh and L. Briand, "A Model-based Conceptualization of Requirements for Compliance Checking of Data Processing against GDPR," 2021 IEEE 29th International Requirements Engineering Conference Workshops (REW), Notre Dame, IN, USA, 2021, pp. 16-20, doi: 10.1109/REW53955.2021.00009.

[13] F. Artuğer and F. Özkaynak, "JPEG Algoritmasının Performansını İyileştirmek İçin Bir Yöntem", Fırat Üniversitesi Mühendislik Bilimleri Dergisi, vol. 34, no. 1, pp. 25–32, 2022, doi: 10.35234/fumbd.865004.

[14] F. Artuğer, F. Özkaynak, Chaotic quantization based JPEG for effective compression of whole slide images. Vis Comput 39, 5609–5623 (2023). https://doi.org/10.1007/s00371-022-02684-y Fırat

[15] S. Singh, M. Rakhra, A. Malik and D. Singh, "Blockchain-based EHR System for Indian Healthcare Industry using Aadhar," 2023 International Conference on Intelligent and Innovative Technologies in Computing, Electrical and Electronics (IITCEE), Bengaluru, India, 2023, pp. 997-1001, doi: 10.1109/IITCEE57236.2023.10091065.

[16] M. Al Baqari and E. Barka, "Biometric-Based Blockchain EHR System (BBEHR)," 2020 International Wireless Communications and Mobile Computing (IWCMC), Limassol, Cyprus, 2020, pp. 2228-2234, doi: 10.1109/IWCMC48107.2020.9148357.

[17] B. J. D. J, S. Sibi Rajan, R. Vibinanth, D. Pamela and P. Manimegalai, "I-Doc – A Cloud Based Data Management System For Health Care," 2022 6th International Conference on Devices, Circuits and Systems (ICDCS), Coimbatore, India, 2022, pp. 85-88, doi: 10.1109/ICDCS54290.2022.9780811

[18] https://www.gartner.com/en/documents/4009215

[19] J. Kim, Y. J. Mo, W. Lee and D. Nyang, "Dynamic Security-Level Maximization for Stabilized Parallel Deep Learning Architectures in Surveillance Applications," 2017 IEEE Symposium on Privacy-Aware Computing (PAC), Washington, DC, USA, 2017, pp. 192-193, doi: 10.1109/PAC.2017.22.

[20] I. E. Ivanov, V. E. Gueorguiev, K. Kassev, L. A. Nenov and D. V. Georgieva, "Regional and national PACS - Structural and security problems," 2021 Sixth Junior Conference on Lighting (Lighting), Gabrovo, Bulgaria, 2021, pp. 1-4, doi: 10.1109/Lighting49406.2021.9599020.

[21] J. Kaberuka and C. Johnson, "Adapting STPA-sec for Socio-technical Cyber Security Challenges in Emerging Nations: A Case Study in Risk Management for Rwandan Health Care," 2020 International Conference on Cyber Security and Protection of Digital Services (Cyber Security), Dublin, Ireland, 2020, pp. 1-9, doi: 10.1109/CyberSecurity49315.2020.9138863.

[22] K. Hovhannisyan, P. Bogacki, C. A. Colabuono, D. Lofù, M. V. Marabello and B. Eugene Maxwell, "Towards a Healthcare Cybersecurity Certification Scheme," 2021 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA), Dublin, Ireland, 2021, pp. 1-9, doi: 10.1109/CyberSA52016.2021.9478255.

[23] A. Mali, A. G. Ororbia, D. Kifer and C. L. Giles, "Neural JPEG: End-to-End Image Compression Leveraging a Standard JPEG Encoder-Decoder," 2022 Data Compression Conference (DCC), Snowbird, UT, USA, 2022, pp. 471-471, doi: 10.1109/DCC52660.2022.00082.

[24] K.R. Rao; Humberto Ochoa Domínguez; Shreyanka Subbarayappa, "15 JPEG Systems," in JPEG Series , River Publishers, 2021, pp.277-278.

[25] X. Huang, S. Wang and G. Liu, "Detecting Double Jpeg Compression with Same Quantization Matrix Based on Dense Cnn Feature," 2018 25th IEEE International Conference on Image Processing (ICIP), Athens, Greece, 2018, pp. 3813-3817, doi: 10.1109/ICIP.2018.8451569.

[26] Y. Niu, X. Li, Y. Zhao and R. Ni, "Detection of Double JPEG Compression With the Same Quantization Matrix via Convergence Analysis," in IEEE Transactions on Circuits and Systems for Video Technology, vol. 32, no. 5, pp. 3279-3290, May 2022, doi: 10.1109/TCSVT.2021.3097351.

[27] G. Wallace, The JPEG still picture compression standard, IEEE Trans Consum Electron 20, 38: 18- 34, 1992.

[28] K. Yamatani and N. Saito, "Improvement of DCT-Based Compression Algorithms Using Poisson's Equation," in IEEE Transactions on Image Processing, vol. 15, no. 12, pp. 3672-3689, Dec. 2006, doi: 10.1109/TIP.2006.882005.