UDC 62-50
DOI: 10.20535/SRIT.2308-8893.2024.1.02

DIGITAL MEDICAL IMAGE ENCRYPTION APPROACH IN REAL-TIME APPLICATIONS

IZZ K. ABBOUD, MUAAYED F. AL-RAWI, NASIR A. AL-AWAD

Abstract. Patient information and medical imaging data are now subject to stringent data security and confidentiality standards due to the proliferation of telemedicine techniques and medical imaging instruments. Because of the problems described above, as well as the possibility of data or information being stolen, this brings up the dilemma of transmitting data on medical images via an open network. In the past, potential solutions included the utilization of methods such as information concealment and image encryption. Nevertheless, attempting to reconstruct the original image utilizing these approaches may result in complications. In the process of this paper, an algorithm for safeguarding medical images based on the pixels of interest was established. Detection of image histogram peaks for the purpose of calculating peaks in medical images pixels of interest in medical image that have had their threshold values processed. The threshold is shown by taking the average of all the peaks in the histogram. After that, a Sudoku matrix is used to assign values of interest to each of these pixels. The proposed method will be assessed by a variety of statistical procedures, and the outcomes of these analyses will be compared to previously established standards. According to the findings, the suggested method has superior security performance compared to other image encryption methods already in use.

Keywords: real time applications, medical images, encryption, security, peak detection.

INTRODUCTION

Because of increased and better investment in multimedia techniques, research pertaining to medical imaging has made great strides forward in recent years. The vital personal information that the patient wishes to keep private is included in the medical image. In order to safeguard sensitive information, medical images are often encrypted. Textual data is often encrypted via one of many standard algorithms, including Advanced Encryption Standard (AES), Data Encryption Standard (DES), International Data Encryption Algorithm (IDEA), or Triple DES. Other frequent encryption techniques include the pixels in medical images are not evenly distributed, and the data has a high resolution. There are also distinct geographical patterns. Due to the slowness of bulk data, traditional encryption is not an appropriate method for safeguarding images from digital imaging and communication systems (DICOM) in the field of medical care.

RELATED WORK

When medical professionals require more information to diagnose a patient, medical imaging provides a secondary source of information that is both vital and effective [1]. Unfortunately, the fastest way to transmit medical images (and the one that is often considered to be the most effective) is typically over open net-

works like sharing files and email. Images that have been sent in this manner are at risk of being subject to actions such as content alteration, illicit duplication, and the loss of copyright [2]. As a direct consequence of this, there has been an increase in the number of studies into medical image security that focus on image encryption and information concealment [3]. The article [4] provided an explanation of an approach that was not only simple but also effective. It included utilizing matrix multiplication to change the pixel values in an image, which resulted in a fairly straightforward process but made it very difficult for unauthorized individuals to extract the information contained in the images. A combination of a logistic map and a 3D Lorenz, both of which displayed multiple operating modes, was essentially what produced the 5-D hyper chaotic map that was mentioned in the study [5]. While one of the modes concentrates only on the pixels that are derived from images with clear text, the other option diffuses the light a total of two times in order to produce images that are secured. Because of the study that solved the security problem [6], it is now possible for online users' sensitive data to be exchanged on web apps without the users' needing to worry about their privacy being compromised. Article [7] developed a 1-D chaotic map in order to get additional security by recognizing its shortcomings. This was followed by the presentation of a modified version of the plain text attack. Paper [8] revealed the hidden data that was hiding in a portion of the image by picking an essential section of a medical image, which is something that is often done by choosing the portions of the image that are utilized more frequently. In article [9], a method for partially encrypting secret data contained in photographs was presented, with FF1 and FF3-1 serving as key components.

The sensitive information will be encrypted without leading to an increase in the file size, which might result in a loss of memory. The gray scale encryption method based on Image Region of Interest (ROI) with chaos is presented in article [10]. To begin, the portion of the ROI that has to be recognized must be done so utilizing the Sobel edge detection technique. The edges of the blocks must then be used to sort the components of the image into those that are significant and those that are not essential. Sine maps are utilized to encrypt the irrelevant area, whereas the Lorenz method is utilized to encrypt the region that contains the ROI. Paper [11] provides a self-generating area of interest (ROI) approach for watermarking applications in biological images. The most significant benefit that this approach has over others is that it is secure enough to avoid a wide variety of attacks, including those using Gaussian, median, sharpening, and wiener filters. Research [12] addressed a new approach in which he showed how to identify the ROI with perfect precision, how to prevent information leakage in the ROI section, and how to retrieve the information lossless from encryption in the transform domain. This approach was presented as part of the discussion of the new approach. Therefore, here we come across a unique lossless game theory based medical image encryption approach with optimal ROI parameters in addition to ROI concealed locations. This method was developed in this work. In order to retrieve the medical picture without losing any data, the process of encryption must first entail a transformation at the pixel level of the ROI. This is done to safeguard the loss of information contained within the medical image. The chaos-based encryption approaches covered in the article [13] make use of a variety of different encryption algorithms. The article [14] suggested an enhanced histogram shifting (HS) reversible watermark technique for medical images and others' work in order to increase the hidden capacity of the algorithm. For the purpose of embedding information utilizing the HS technique, an image should be cut up into

smaller parts. The authors of article [15] place a high priority on integrating information into texture regions via the use of HS and contrast enhancement, with the goals of enhancing contrast in texture areas and improving how the image is subjectively perceived. In the study by [16], the authors preserved patient information by using a reversible image masking strategy for HS. After that, they enhance image quality by using two parameters of linear prediction: weight and threshold. The economy and the interest rate merged. Research [17] suggests using an HS technique to look into the lossless data that high-resolution medical images conceal. Employ a strong correlation in the image's local block pixels for the purpose of rendering the smooth surface of the medical imaging anatomy. It is not difficult at all to modify the capacity and the signal-to-noise ratio (PSNR) in accordance with the block size, the partition level, and the number of embedded bits. Many of the objectives of the aforementioned approaches include ensuring that the image is protected from infringement on its copyright and minimizing the amount of distortion in the visual quality of the embedded image. Image histogram peak detection is a basic approach for digital image processing that may be used directly and efficiently for image segmentation, quality evaluation, enhancement, decrease in data, and other purposes. It is also one of the most important aspects of digital image processing.

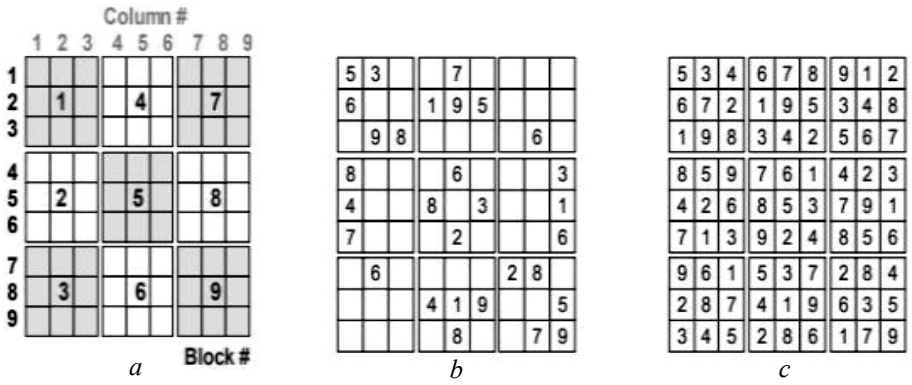


Fig. 1. A sample Sudoku puzzle and its solution: *a* — Row#, Column # and Block# notation; *b* — a sample Sudoku puzzle; *c* — the solution to Sudoku puzzle (*b*)

SUDOKU MATRIX

A Sudoku matrix is denoted by the notation $X \times X$ and may include any number between 1 and N. However, given that X is the square of the number and N equals X, each number can only appear once in each row of the matrix. Only the first value in each column and the first value in each block will be increased. The following illustration in Fig. 1 provides a sample of a Sudoku problem as well as the answer for $X = 9$. The result of successfully solving a Sudoku problem is referred to as the "Sudoku matrix".

Sudoku Typical Sudoku problems are derived from the Sudoku Matrix by omitting some cells, but each problem also includes hints on how to solve it on its own. The researchers have made an effort to come up with a number of different solutions. In this piece, we will construct a Sudoku matrix via the use of a technique called the Latin square. The downside of this rapid and systematic technique is that the set of Sudoku matrices that it generates is just a subset of the universal set of all possible Sudoku matrices. This is a limitation of the method, but it does not prevent it from being useful.

PROPOSED ENCRYPTION SELECTIVE METHOD

Fig. 2 presents the block diagram of the proposed selective image encryption method. The proposed method is comprised of a number of processes that, in order to identify and encrypt the area of interest in the medical image, are necessary. The first step is to calculate the histogram peak of the original image using the formula presented in Fig. 3. The peak detection method uses the image histogram to first create a peak detection signal. The extrema that are between the zero and zero intersections of the peak detection signal are then used in order to locate the peaks that are present in the histogram. A close approximation of the first derivative may be achieved using convolution by utilizing a differentiator. The peak may be identified in a histogram that has ideal smoothness by locating the point where the sign and zero intersection of the signal that was produced by the h and S convolutions occur. The extrema of the histogram and the location of the turning point may be estimated using the zero intersection method. The peak values of the original medical imaging are shown by the symbol "*" in Fig. 3. The threshold value for separating the relevant pixels in a medical image may be derived by taking the average of all the peak values that are acquired via the use of the histogram peak detection function. The next step is to examine each pixel in the original medical image against the predetermined threshold value; if the value is higher, the pixels must be grouped together to form a meaningful pixel block. The diffusing procedure is performed on a Sudoku matrix consisting of numerous random 16*16 grids. Perform an XOR operation on the significant pixel block using the pixels in the Sudoku matrix to generate a random encryption of the block.

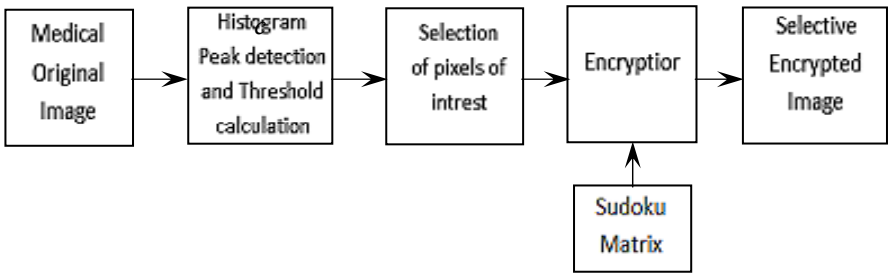
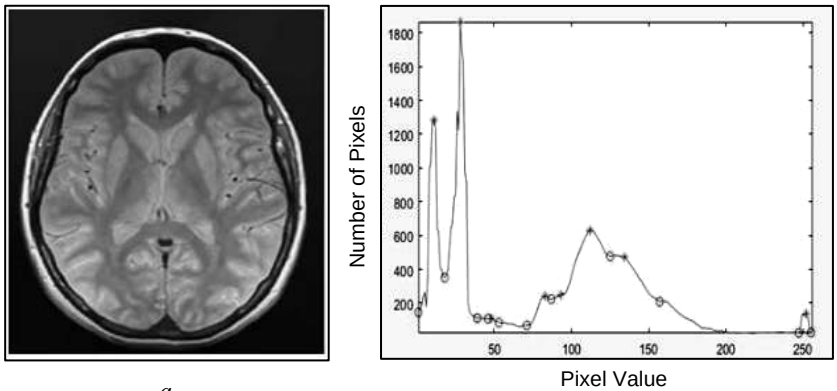


Fig. 2. The architecture of proposed visible image encryption method



a *b*

Fig. 3. Original MRI image — *a*; Peak detection using histogram — *b*

SIMULATION AND RESULT DISCUSS OF THE PROPOSED METHOD

By simulating the proposed encryption selective method on a PC using MatLab, images are transferred after the medical image has been encrypted. When transferring the medical image, we transfer the encrypted image to protect the original medical image. This is possible because the only person who will be able to view the original after this process is the person to whom we want to transfer the image. After the decryption procedure of the encrypted medical image, the original image is only sent to that specific person. Fig. 4 displays the original Magnetic Resonance Imaging (MRI) with its encryption image. Once an image has been encrypted, the original image cannot be reconstructed until the encryption process has been completed correctly. In a similar fashion, Fig. 5 and Fig. 6 display the original image as well as the encrypted version of the hand and leg images respectively.

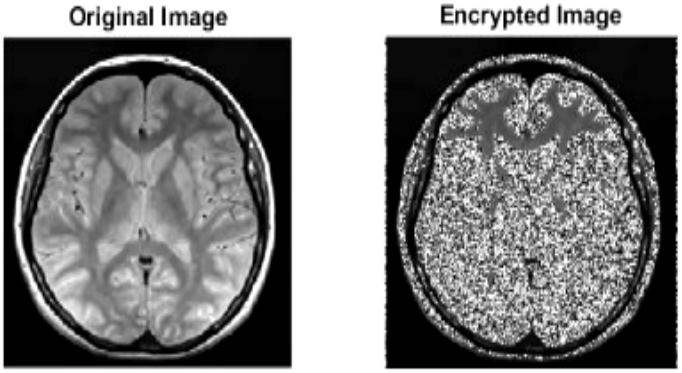


Fig. 4. The input MRI image and corresponding ROI encrypted MRI image

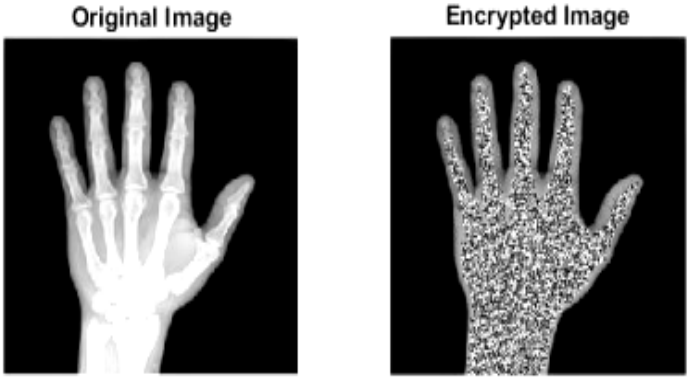


Fig. 5. The input hand image and corresponding ROI encrypted hand image

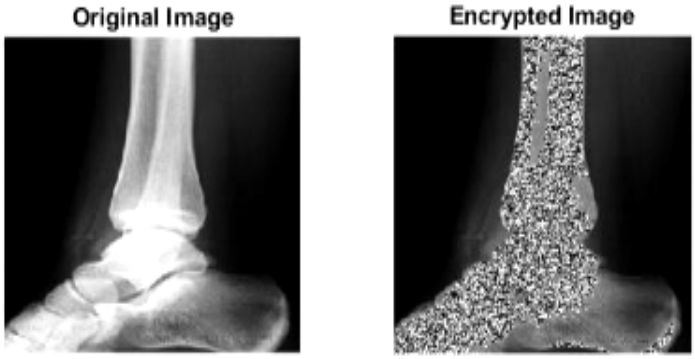


Fig. 6. The input leg image and corresponding ROI encrypted leg image

CONCLUSION

In this paper, we present a method for partially encrypting personal data, such as tumors in the brain, hand parts, and so on. Padding and a rise in data volume as a result of wasted storage space over time are challenges that are inherent to traditional image protection systems. Additionally, since the whole image is encrypted, it cannot be recognized before it is decrypted, and when it is decrypted, critical information is revealed. The difficulty with conventional sub-image encryption is that it encrypts superfluous sections by first encrypting a rectangular region that covers information that has to be kept private. This issue can now be resolved via the technique that was suggested. The suggested approach encrypts the data using a Sudoku matrix after it has been used to determine the important pixels using a histogram peak detection approach.

REFERENCES

1. B. Thomee, D.A. Shamma, and G. Friedland, "YFCC100M: The New Data in Multimedia Research," *Communications of the ACM*, vol. 59, no. 2, pp. 64–73, 2015.
2. S. Pouyanfar, Y. Yang, and S.C. Chen, "Multimedia Big Data Analytics: A Survey," *ACM Computing Surveys*, vol. 51, no. 1, pp. 1–34, 2018.
3. Y. Sun, S. Fang, and Y. Hwang, "Investigating Privacy and Information Disclosure Behavior in Social Electronic Commerce," *Sustainability*, vol. 11, no. 12, pp. 1–27, 2019.
4. M. Han, L. Li, and Y. Xie, "Cognitive Approach for Location Privacy Protection," *IEEE Access*, vol. 6, pp. 13466–13477, 2018.
5. S. Liu, C. Guo, and J.T. Sheridan, "A review of optical image encryption techniques," *Optics & Laser Technology*, vol. 57, pp. 327–342, 2014.
6. Y. Dai, H. Wang, and Z. Zhou, "Research on medical image encryption in telemedicine systems," *Technology and Health Care*, vol. 24, no. s2, pp. S435–S445, 2016.
7. G. Chen, Y. Mao, and C. Chui, "A symmetric image encryption based on 3d chaotic cat maps," *Chaos, Solitons Fractals*, vol. 21, pp. 749–761, 2018.
8. R. Enayatifar, A.H. Abdullah, and I.F. Isnin, "Chaos-based image encryption using a hybrid genetic algorithm and a DNA sequence," *Optics and Lasers in Engineering*, vol. 56, pp. 83–93, 2014.
9. Ü. Çavuşoğlu, S. Kaçar, A. Zengin, and I. Pehlivan, "A novel hybrid encryption algorithm based on chaos and S-AES algorithm," *Nonlinear Dynamics*, vol. 92, pp. 1745–1759, 2018.
10. J. Wu, X. Liao, and B. Yang, "Color image encryption based on chaotic systems and elliptic curve EIGamal scheme," *Signal Processing*, vol. 141, pp. 109–124, 2017.
11. C. Paar, J. Pelzl, *Understanding cryptography: a textbook for students and practitioners*. Springer Science & Business Media, 2009.
12. Z. Su, G. Zhang, and J. Jiang, "Multimedia security: a survey of chaos based encryption technology," in *Multimedia-A Multidisciplinary Approach to Complex Issues*, *InTech*, pp. 99–124, 2012.
13. T. Xiang, S. Guo, and X. Li, "Perceptual visual security index based on edge and texture similarities," *IEEE Transactions on Information Forensics and Security*, vol. 1, no. 5, pp. 951–963, 2016.
14. M. Noura, H. Noura, A. Chehab, M.M. Mansour, L. Sleem, and R. Couturier, "A dynamic approach for a lightweight and secure cipher for medical images," *Multimedia Tools and Applications*, vol. 77, no. 23, pp. 31397–31426, 2018.

15. M. Li, D. Lu, and W. Wen, “Cryptanalyzing a color image encryption scheme based on hybrid hyper-chaotic system and cellular automata,” *IEEE Access*, vol. 6, pp. 47102–47111, 2018.
16. L. Xu, Z. Li, and J. Li, “A novel bit-level image encryption algorithm based on chaotic maps,” *Optics and Lasers in Engineering*, vol.78, pp. 17–25, 2016.
17. L. Teng, X. Wang, and J. Meng, “A chaotic color image encryption using integrated bit-level permutation,” *Multimedia Tools and Applications*, vol. 77, no. 6, pp. 6883–6896, 2018.

Received 16.06.2023

INFORMATION ON THE ARTICLE

Izz K. Abboud, ORCID: 0000-0002-8344-8585, Mustansiriyah University, Iraq, e-mail: izz_kadhum@uomustansiriyah.edu.iq

Muaayed F. Al-Rawi, ORCID: 0000-0003-1841-1222, Mustansiriyah University, Iraq, e-mail: muaayed@uomustansiriyah.edu.iq

Nasir A. Al-Awad, ORCID: 0000-0003-3059-4375, Mustansiriyah University, Iraq, e-mail: nasir.awad@uomustansiriyah.edu.iq

ШИФРУВАННЯ ЦИФРОВИХ МЕДИЧНИХ ЗОБРАЖЕНЬ У ПРОГРАМАХ РЕАЛЬНОГО ЧАСУ / Ізз К. Аббуд, Муаайед Ф. Аль-Раві, Насір А. Аль-Авад

Анотація. Інформація про пацієнтів і дані медичних зображень тепер підпадають під дію суворих стандартів безпеки даних і конфіденційності, що є прямим результатом поширення телемедичних методів й інструментів для медичних зображень. Через зазначені проблеми, а також через можливість викрадення даних або інформації, виникає дилема передавання даних на медичні зображення через відкриту мережу. У минулому потенційні рішення включали в себе використання таких методів, як приховування інформації та шифрування зображень. Тим не менше спроба реконструювати оригінальне зображення за допомогою цих підходів може призвести до ускладнень. У ході роботи створено алгоритм для захисту медичних зображень на основі пікселів інтересу. Виявлення піків гістограми з метою обчислення піків у медичних зображеннях пікселів інтересу медичних зображеннях, для яких оброблені порогові значення. Порогове значення відображається як середнє значення усіх піків на гістограмі. Після цього застосовується матриця Sudoku для призначення значень інтересу кожному з цих пікселів. Запропонований метод оцінено за допомогою різноманітних статистичних процедур, а результати цих аналізів порівняно з раніше встановленими стандартами. Згідно з висновками, запропонований метод має кращу ефективність безпеки порівняно з іншими вже використовуваними методами шифрування зображень.

Ключові слова: додатки реального часу, медичні зображення, шифрування, безпека, виявлення піків.