NFSU JOURNAL OF CYBER SECURITY & DIGITAL FORENSICS

NFSU – Journal of Cyber Security and Digital Forensics
Volume – 1, Issue – 1, December 2022
E – ISSN – 2583-7559

RECENT TRENDS IN MEDICAL IMAGE AUTHENTICATION ANDENCRYPTION

Param Ahir, Mehul Parikh

Computer Department
Gujarat Technological UniversityAhmedabad, India param.ahir@nfsu.ac.in

Information Technology Department
L. D. College of EngineeringAhmedabad, India
mehulcparikh@ldce.ac.in

***Abstract*— Medical and diagnostic imaging fields have significantly benefited from technological advancements. Several methods are being used to improve and generate higher- quality images, and efforts are being made to develop an artificial intelligence-based solution for autonomous disease prediction from medical images. The medical field rapidly adapts to telemedicine, allowing patients to receive care from remote locations. As a result of these medical advancements, the need to send medical images across a network has grown exponentially, as have the challenges of doing so securely. These images contain susceptible and personal health-related records of a patient, and any manipulation of these images will result in incorrect predictions and, ultimately, the wrong course of treatment. Various encryption and watermarking techniques are used to secure these images. In this paper, we critically reviewed recent developments and trends in medical image security.**

Keywords—Medical Imaging, Cyber security, Data Confidentiality, Authentication, Encryption, Image Watermarking

I. INTRODUCTION

In today's world, there has been an increase in the transmission of various types of medical records via the internet. This is mainly due to the advent of telemedicine, the limited availability of experts in the surrounding area, the need to conduct various experiments and research in medicine, and the demand for e-healthcare and electronic medical records systems. As a result of these factors, medical records are typically stored in the cloud and made available to users upon request. This patient's medical history must be safeguarded to protect the data contained within it and ensure that individual patient records are kept confidential. In several countries, it is against the law to use or disclose a person's medical information without first obtaining their consent. Unauthorized disclosure of medical information in these parts of the world could have serious legal ramifications. Medical image processing is a critical task in the field of medicine. Medical image processing is used to determine the underlying causes of diseases and potential treatments. These images are generally stored, processed, and transmitted through cloud storage over the internet. The primary challenges that arise during the transmission, storage, and processing of medical images in such a distributed environment are (i)image authentication and (ii) secure image transmission. A variety of watermarking techniques are used to authenticate images. Many encryption methods are used to protect medical images. This paper focuses on recent advancements in these techniques and identifies research gaps to assist researchers working in the field.

Deep learning has demonstrated strong performance in computer vision and, more specifically, medical image analysis. Using deep learning to automate specific medical tasks produces superior results, but it also leads to adversarial attacks. These cyberattacks involve making a very small but significant change to the machine learning model's input. This modification is undetectable to humans, but it results in substantial errors in the model's desired output. Many of the most recent and cutting-edge models have historically provided inaccurate predictions when given such altered inputs. When it comes to medical images, even seemingly insignificant changes can cause havoc for the systems and the professionals who use them. Once an attack has been carried out, it is difficult to detect, localize, and recover the region tampered with, making it critical to protect images against any type of attack.

The challenge of protecting medical images is not only critical, but it is also frequently difficult. Because these decision-making tools are so essential to health professionals, the system for protecting medical images must be as robust as possible. Techniques such as image transformation-based malware classification, image deblurring, image encryption, image watermarking techniques, and others are used to ensure the secure transmission of medical images; however, there is significant scope for improvement in this area. One of the most critical challenges in transferring medical images over a wireless network is authenticating these images. Medical image authentication systems' primary goals are to prevent images from being tampered with and to confirm that they have not been altered in any way. Authenticating images frequently necessitates the use of several different digital watermarking strategies. The issue with these technologies is that they have the potential to cause persistent aberrations in the image, which can lead to incorrect medical diagnoses. For medical image authentication, various reversible watermarking[17] and zero watermarking[18] systems are used. Another method to authenticate is through

encryption. Medical image encryption is complex and cannot be accomplished using standard data encryption techniques designed for textual data. This is because medical images have a higher degree of pixel correlation than regular images, have a higher volume, and contain a lot of redundant information.

The paper is broken up into five distinct sections. The first component of the paper consists of some general background information on the topic. It provides a description of the authentication and encryption processes that were previously utilized for medical images. In the second part of this paper, we will explore various methods that have lately been employed for the authentication of medical images. In the third part of this article, we will go through recent methods for encrypting medical images. The evaluation metrics for encryption and authentication methods are listed in the fourth section. In the fifth section, we explore the future research gaps and future scope for this field. By conducting this literature review, we are investigating all of the different methods currently available for authenticating and encrypting medical images, as well as potential future work in this area.

II. RELATED WORK

X-ray, computed tomography (CT) scans, magnetic resonance imaging (MRI), and ultrasound are all forms of imaging that are utilized in making a general medical diagnosis. Each sort of medical image helps in the detection of ailment and is created through the use of a unique technological process. Because of the growing variety of imaging types, medical personnel now have a wide variety of alternatives at their disposal for illustrating what is happening on the inside of a patient's body. These pictures are saved and sent across the network for use in a wide variety of applications, including telemedicine, automatic feature selection, image correction, denoising, automatic segmentation, and many more. These hospital network routes are frequently extremely ill-protected and open to the possibility of cyber-attacks. These types of attackers can obtain patient health information as well as make changes to these images, which can result in an incorrect diagnosis. Because of this, it is essential to ensure that images come from an authenticated source and that no one other than the user who intended to read or acquire this data can do so. Medical image authentication and medical image encryption are the two primary topics to focus on in this regard.

A. Medical Image Authentication

In cyber security and image processing, authentication has been and will continue to be essential because images are being transferred over an unsecured network. The medical image authentication mechanism helps to ensure that the integrity of the images is maintained. For image authentication, several different cryptographic, hashing, and watermarking approaches are utilized. These methods need some modification before they can be used effectively with medical images. Specific fundamental characteristics need to be taken into account to authenticate medical images. These features include the fact that medical images have a large volume and are extremely sensitive to distortions, both of which have the potential to alter the diagnosis that is derived from these images. When it comes to the development of medical image authentication methods, this system is required to include several explicit qualities. The system needs to be sensitive to image alterations and instantly detect them when they occur. When utilizing methods such as watermarking, care should be taken to guarantee that the image's content is not altered. It is necessary to have the mechanism for image localization and restoration. Earlier research in this field focused mainly on techniques[19] including machine authentication codes, manipulation detection codes, digital signatures, and hashing. The inability to pinpoint precisely where manipulation is taking place is one of the most significant limitations associated with techniques based on cryptography. The use of watermarking on medical images is yet another essential authentication technique. The process of watermarking an image can be completed using one of four distinct methods[22]: visible watermarking, invisible watermarking, dual watermarking, or fragile watermarking. The ability to store patient details within the image is one of the primary advantages of utilizing the watermarking technique. Another advantage is the reduced bandwidth requirements for data transmission, which is made possible by the fact that patient metadata is concealed within the image in the form of a watermark. If watermarks are correctly implemented it can act as keyword for image storing and retrieval module. In the past, well-known watermarking techniques used correcting codes and procedures involving machine learning. In addition to these another method such as biometric and compression-based one, were developed. One of the most significant issues with older methods was that they caused the original image to become distorted, and this issue could not be fixed after it had been transmitted. When it comes to medical images, this can lead to inaccurate diagnoses, which can then result in patients receiving inappropriate treatments. All medical image watermarking techniques must ensure that the procedure does not degrade image quality and that confidential patient details embedded within images can be extracted without errors during decompression. Watermarking techniques currently used can be classified in the spatial and transform domains. The following section of the paper gives details about these techniques.

B. Medical Image Encryption

Medical images are highly vulnerable to cryptographic attacks when they are transmitted through an unsecured network connection. The three primary security objectives are confidentiality, integrity, and availability. Among these three considerations, the confidentiality of medical images is the most important. Encryption of medical images is used to protect patient's private medical images. To prevent unauthorized access to medical images, an encryption method involving the randomization of image pixels is used. Encrypting data is widely regarded as one of the most effective techniques in the field of cryptography. The two primary classifications of this technology are symmetric and asymmetric encryption methods. The symmetric encryption method uses a single key for both the ciphering and decoding processes. In asymmetric encryption, the encryption process is performed using the receipt's public key, and receipts can decrypt information using their private keys. Encrypting medical images is done using various techniques including

bitwise XOR diffusion, edge maps, chaotic maps, and high-speed scrambling. Certain characteristics, such as the ability to protect the medical images integrity and confidentiality, are maintained through medical image encryption. This can be accomplished by ensuring that the images are not corrupted during transmission and that they are safe from cyberattacks and other forms of danger. Methods that have been shown to be very effective with textual data, such as the Data Encryption Standard (DES), the Advanced Encryption Standard (AES)[15], and the International Data Encryption Algorithm (IDEA)[16], are not suitable for use with digital images due to the high degree of redundancy and correlation between the pixels in images. Some methods of digital image encryption encrypt images by interleaving specific bits from the pixel values in images; however, these methods cannot be used for medical images because they result in significant data loss, some of that lost data potentially important for diagnosis. In order to encrypt images, certain methods specify the chain of cypher blocks with the stream data. These methods do not work well with large amounts of data, so they cannot be used with some types of medical images, such as MRI and CT-SCAN, which produce large images. Specific strategies have been developed in recent years to overcome all of these challenges; these strategies will be discussed in the following section.

III. VARIOUS TECHNIQUES FOR MEDICAL IMAGE AUTHENTICATION

In recent years, a significant number of efficient techniques have been developed in the field of medical image authentication. Most of the recent noteworthy work in medical image authentication is based on watermarking. Several different mathematical equations are combined in order to generate a one-of-a-kind authentication marking on an image while simultaneously concealing patient details inside the image itself. Most of the work is on ensuring that the watermark can be extracted effectively and that the image generated by the technique is of excellent quality and free of any distortions. This is because these two factors are essential to the success of the approach. The following sections will provide an overview of each of these approaches in further depth.

A. Medical Image Watermarking with patient's fingerprint[1]

In this method, they present a watermarking method that uses hybrid features derived from the Lifting Wavelet Transform (LWT), the Discrete Wavelet Transform (DWT), and the Local Binary Pattern (LBP). The patient's fingerprint is used as a key to add a watermark to the image. The LBP values are included in the key along with the fingerprint. The Arnold transform is used to provide three levels of security. This method is quite dependable, and it provides a high level of security by attaching user personal identification details that are unique to each individual user.

B. Reversible Medical Image Watermarking with Image Scaling [2]

In this method hybrid approach is implemented by, combining reversible watermarking and zero watermarking techniques. This technique is three times quicker than other watermarking methods because it creates a watermarked image by performing a scaling operation on the actual image. This is one of the most significant benefits of this method, as it eliminates the need for a separate procedure. Using this technique results in an image of exceptionally high quality. This method also contained a methodology for determining whether or not an image has been altered in any way. To deactivate the watermark and gain access to the image, the procedure generates a unique authentication code that the user must input into the system to get the original image back once it is watermarked.

C. MiniEigen Value-based blind watermarking for MedicalImages [3]

The MiniEigen Value is used in this technique to generate the image's feature map bits. By combining the chaotic sequence method with Quantization Index Modulation, the method is made real-time and significantly more secure. This method is known as blind watermarking because data embedded inside an image can be recovered using the key used during the embedding phase even if the original image is not present.

D. Fragile watermarking with self-recovery and tampering with medical images [4]

This strategy makes use of Turtle Shell-based Hiding (TSDH). Authentication codes and recovery information are both created in a distinct method using this approach. The generation of a weighted watermarked image includes taking the original image and a block of pixels measuring 2 X 2 and averaging the results to create self-recovery information. For the purpose of producing authentication codes, the Principal Component Analysis (PCA) approach is utilized. The ability of this technology to restore the original image, even after one or more attackers have altered it, is one of its most significant advantages.

E. Medical Image Tamper detection using Enhanced Neighbor Mean Interpolation (ENMI) technology[5]

This method expands original images by adding a 2X2 block to original 3X3 block images using enhanced neighbor mean interpolation. By combining the data hiding mechanism provided here with the authentication code, this strategy was able to incorporate patient data into the image. In this case, four pixels from the image's corners are left unchanged, while an ENMI interpolation algorithm is used to generate five more pixels. Four of the five pixels contain sensitive data, while the fifth contains an authentication code.

F. CT-SCAN authentication using predication-based reversible watermarking[6]

This method is primarily concerned with recovering the region of interest that has been tampered during transmission and producing high-quality watermarked images. On CT-SCAN, this method employs reversible watermarking. It employs a distinct watermark strategy for the Region of Interest (ROI) and the Region of Non-interest (RONI). The fragile watermarking technique is used on ROI, while the composite watermarking technique is used on RONI.

G. Medical Image Authentication using DWT-based watermarking[7]

This method includes patient information in the image's Discrete Wavelet Transform (DWT) coefficient. This method applies blind watermarking, in which the original image is not

required for watermark extraction. A hash embedded in the image is compared to ensure that the extracted patient information is correct. One of the primary advantages of this model is that it can handle large amounts of data.

H. Medical Image watermarking through DWT and SVT[8]

This paper creates a watermark by selecting a fuzzy-based Region of Interest and then transforming the wavelength. The image is sent through a fuzzification module to determine the region of interest, which identifies significant positions in the image. The watermarked image is then decomposed using wavelet decomposition and sent to the time-frequency domain. It is dependable and highly secure due to the presence of two layers of watermarking. This method is capable of achieving high embedding rates while causing minimal image distortion.

IV. VARIOUS TECHNIQUES FOR MEDICAL IMAGE ENCRYPTION

Research in cryptography has traditionally focused a lot of attention on encryption because of its significance. In recent years, the field of medical image encryption has seen significant progress, with the development of a wide range of effective new approaches. Deep learning, genetics, chaotic maps, and other similar approaches have been used in the majority of recent work in the field of medical image encryption. The development of an extremely trustworthy encryption model requires the integration of several various disciplines. The following are some of the more recent approaches used in the field.

A. Medical Image Encryption with Stream Cipher Generator[9]

In this method, private keys are generated by using the generative adaptive network (GAN). These private keys are used in the encryption and decryption processes. This method is based on the idea that if the style of the desired private key is known, that style can be used as the transformation domain of GAN. The bit-wise XOR algorithm is used as an encryption and decryption algorithm. This method is susceptible to change and can withstand various attacks due to its one-time pad method, large key space, and pseudo-randomness.

B. Medical Image Encryption using DNA Code and chaoticmap[10]

A combination strategy of SHA-2 hashing, chaotic map, and deoxyribonucleic acid masking (DNA) is used to create the encryption algorithm for this method. In this method, the color image is encoded using DNA coding. The chaotic map function of this encryption technique is the most important part of it because it is used in the diffusion process. This method generates keys using the SHA-2 technique. Because of the hybrid approach used, this technique is both secure and fast.

C. Medical Image Encryption using hybrid DNA Computingand chaos transformation domain[11]

The encryption algorithm in this method implements a hybrid model based on integer wavelet transform (IWT) and deoxyribonucleic acid (DNA). The algorithm is broken up into two distinct stages: the shuffling stage, and the diffusion stage. During the shuffling phase, the bits of the image are shifted in a bitwise manner, and during the diffusion phase, a DNA XOR operation is carried out. This method's high-performance level can be attributed to the dual layer of protection that Method provides.

D. Medical Image Encryption using Field Programmable Gate Array [12]

This approach uses a complex chaos-based Pseudorandom Number Generator (PRNG) and a medical image encryption algorithm based on the Modified Advanced Encryption Standard (MAES). It uses shift-rows permutation and mix-columns permutation, both of which contribute to the high complexity of the system too reduce the time complexity. It only encrypts images using four different rounds. This approach delivers high levels of complexity and randomness while simultaneously providing low time complexity.

E. Medical Image Encryption using the three-leaf chaotic system and genetic operation [13]

In this method, the basic idea behind DNA recombination is linked with the functioning of a five-dimensional three-leaf chaotic system to produce a chaotic matrix. During the diffusion step, a bit-level DNA mutation operation is carried out in order to improve the effectiveness of the subsequent scrambling stage. This method enhances security and generates a significant amount of random information for key generation.

F. Lightweight Medical Image Encryption Technique[14]

This method's primary objective is to reduce the amount of storage space necessary for an encrypted image and the space needed to generate such images. The Hyper Image Encryption Algorithm(HIEA) is utilised in this strategy. The solution that has been proposed is able to adequately secure the images in the Internet of Things while at the same time taking up a very minimal storage space.

V. EVALUATION METRICS

Several evaluation metrics can be used in Medical Image Authentication. These metrics are detailed in Table I.

TABLE I. EVALUATION METRICS FOR MEDICAL IMAGE AUTHENTICATION

Metric	**Details**
Accuracy	Accuracy measures how close a value is to theground truth.
Similarity Ratio	The similarity between the original image andwatermarked image
Time Complexity	Amount of time required to include the watermark and to exclude it afterward.
Security	Amount of time required to break the watermark.
Payload Capacity	Allowed size of Watermark
Peak Signal-to-Noise Ratio (PSNR)	Maximum signal-to-noise ratio in the image
Mean Square Error (MSE)	Mean square error between the original imageand watermarked image
Bit Correct Ratio (BCR)	The ratio of correctly extracted bits from totalembedded bits

Structural Similarity Index Measure (SSIM)	Structural similarity between two modified images.
Normalized Cross-Correlation	The similarity between the original and recovered image

Several evaluation metrics can be used in Medical Image Encryption. These metrics are detailed below in table II.

TABLE II. EVALUATION METRICS FOR MEDICAL IMAGE ENCRYPTION

Metric	**Details**
Time complexity Analysis	Time required for encryption and decryption
Key Sensitivity Analysis	Pixel by pixel comparison between two encrypted images
Key Space Analysis	Number of keys present in critical space set
Statistical Analysis	Statistical analysis through histogram and correlation coefficient of encrypted image pixels
Differential Analysis	Amount of modification required in encrypted image after modification in private key

VI. DISCUSSION AND FUTURE WORK

PSNR and SSIM are the most critical parameters considered during the medical image authentication process. In medical image authentication, there is a primary need for additional research on reversible watermarking technology. Most currently available methods cannot extract the correct image, which might lead to an increased number of incorrect diagnoses. Additionally, the majority of the current techniques are unable to deliver satisfactory outcomes for reversible watermarking. Current approaches can identify regions that have been tampered with, but they cannot self-recover; this is something that can be worked on in the future. More work is required to improve the quality of the watermarked image.

In the field of medical image encryption, in addition to the evaluation metrics discussed previously, there are two additional. The Number of Pixel Change Rate (NPCR) and the Unified Average Changing Intensity (UACI) are the two metrics that are used to generate secret keys. NPCR is the pixel difference ratio in the same ROI between the original image and the encrypted version. The UACI notation is used to indicate the degree of the intensity change. The hybrid chaotic map and DNA code [10] produce the best results out of all of the methods that were investigated. It is secure in addition to being efficient. The primary focus of future work related to this study will be on techniques based on the Advanced Encryption Standard (AES) for key generation and encryption, with the goals of achieving better security and tamper resistance. The speed of encryption and decryption can be increased by utilizing FPGA in a manner that is expanded to employ parallelism in the [11] technique. Aside from that, the majority of approaches are unable to defend against adversarial attacks made on images and the machine learning models that utilize them.

VII. CONCLUSION

When it comes to the protection of medical data that is stored online, two of the most important requirements are medical image authentication and medical image encryption. Since an increasing number of patients and hospitals are opting to keep their medical records online and make use of telemedicine, it is critical that this medical data is protected from all forms of cyber assaults and that the privacy of patient information is maintained. Compared to other forms of textual data and even other forms of visual data, medical images are more complicated because medical images contain complex structures, big sizes, and greater connections than other types of data. Recent advancements in deep learning, genetic algorithms, and chaotic maps have led to the development of very reliable and effective systems of authentication and encryption. Some of the future work is defined in the previous section. The findings of this literature study led us to conclude that the security of medical images is still an emerging field, and additional effort is required to achieve favorable results in this area.

REFERENCES

[1] Vaidya, S. P. (2022). Fingerprint-based robust medical image watermarking in hybrid transform. The Visual Computer, 1-16.

[2] Malayil, M. V., & Vedhanayagam, M. (2021). A novel image scaling based reversible watermarking scheme for secure medical image transmission. ISA transactions, 108, 269-281.

[3] Soualmi, A., Alti, A., & Laouamer, L. (2021). A novel blind watermarking approach for medical image authentication using MinEigen value features. Multimedia Tools and Applications, 80(2), 2279-2293.

[4] Su, G. D., Chang, C. C., & Lin, C. C. (2020). Effective self-recovery and tampering localization fragile watermarking for medical images. IEEE Access, 8, 160840-160857.

[5] C. -C. Lin, C. -C. Chang, W. -J. Kao and J. -F. Chang, "Efficient Electronic Patient Information Hiding Scheme With Tamper Detection Function for Medical Images," in IEEE Access, vol. 10, pp. 18470- 18485, 2022, doi: 10.1109/ACCESS.2022.3144322.

[6] 6. N. A. Memon and A. Alzahrani, "Prediction-Based Reversible Watermarking of CT Scan Images for Content Authentication and Copyright Protection," in IEEE Access, vol. 8, pp. 75448-75462, 2020, doi: 10.1109/ACCESS.2020.2989175.

[7] Kahlessenane, Fares, Amine Khaldi, Redouane Kafi, and Salah Euschi. "A DWT based watermarking approach for medical image protection." Journal of Ambient Intelligence and Humanized Computing 12, no. 2 (2021): 2931-2938.

[8] Balasamy, K., & Suganyadevi, S. (2021). A fuzzy based ROI selection for encryption and watermarking in medical image using DWT and SVD. Multimedia tools and applications, 80(5), 7167-7186.

[9] Ding, Y., Tan, F., Qin, Z., Cao, M., Choo, K. K. R., &

Qin, Z. (2021). DeepKeyGen: a deep learning-based stream cipher generator for medical image encryption and decryption. IEEE Transactions on Neural Networks and Learning Systems.

[10] Guesmi, R., & Farah, M. A. (2021). A new efficient medical image cipher based on hybrid chaotic map and DNA code. Multimedia tools and applications, 80(2), 1925-1944.

[11] Ravichandran, D., Banu S, A., Murthy, B. K., Balasubramanian, V., Fathima, S., & Amirtharajan, R. (2021). An efficient medical image encryption using hybrid DNA computing and chaos in transform domain. Medical & Biological Engineering & Computing, 59(3), 589-605.

[12] Hafsa, A., Gafsi, M., Malek, J., & Machhout, M. (2021). FPGA implementation of improved security approach for medical image encryption and decryption. Scientific Programming, 2021.

[13] Liang, Z., Qin, Q., Zhou, C., Wang, N., Xu, Y., & Zhou, W. (2021). Medical image encryption algorithm based on a new five-dimensional three-leaf chaotic system and genetic operation. PloS one, 16(11), e0260014.

[14] Hasan, M. K., Islam, S., Sulaiman, R., Khan, S., Hashim, A. H. A., Habib, S., ... & Hassan, M. A. (2021). Lightweight encryption technique to enhance medical image security on internet of medical things applications. IEEE Access, 9, 47731-47742.

[15] Alabaichi, A., & Salih, A. I. (2015, October). Enhance security of advance encryption standard algorithm based on key-dependent S-box. In 2015 Fifth International Conference on Digital Information Processing and Communications (ICDIPC) (pp. 44-53). IEEE.

[16] Basu, S. (2011). International data encryption algorithm (Idea)–a typical illustration. Journal of global research in Computer Science, 2(7), 116-118.

[17] Thodi, D. M., & Rodríguez, J. J. (2007). Expansion embedding techniques for reversible watermarking. IEEE transactions on image processing, 16(3), 721-730.

[18] Zhou, Y., & Jin, W. (2011, July). A novel image zero-watermarking scheme based on DWT-SVD. In 2011 International Conference on Multimedia Technology (pp. 2873-2876). IEEE.

[19] Feistel, H., Notz, W. A., & Smith, J. L. (1975). Some cryptographic techniques for machine-to-machine data communications. Proceedings of the IEEE, 63(11), 1545-1554.

[20] Thabit, R. (2021). Review of medical image authentication techniques and their recent trends. Multimedia Tools and Applications, 80(9), 13439-13473.

[21] Vyas, C., & Lunagaria, M. (2014, December). A review on methods for image authentication and visual cryptography in digital image watermarking. In 2014 IEEE International Conference on Computational Intelligence and Computing Research (pp. 1-6). IEEE.

[22] Singh, A. K., Kumar, B., Singh, G., & Mohan, A. (2017). Medical image watermarking. Springer Science+ Business Media.

[23] Suetens, P. (2017). Fundamentals of medical imaging. Cambridge university press.

[24] Beutel, J., Kundel, H. L., Kim, Y., Van Metter, R. L., & Horii, S. C. (2000). Handbook of medical imaging (Vol. 3). Spie Press.

[25] Zhang, B., Rahmatullah, B., Wang, S. L., Zaidan, A. A., Zaidan, B. B., & Liu, P. (2020). A review of research on medical image confidentiality related technology coherent taxonomy, motivations, open challenges and recommendations. Multimedia Tools and Applications, 1-40.