International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

A Critical Analysis of Compression Encryption of Medical Images

Neeraj Giri[1], *Dr. Aakriti Jain*[2], *Dr. Kalpana Rai*[3]

[1, 2,3] Sagar Institute of Research & Technology-Excellence, Bhopal, India

ABSTRACT

The quantity of data pertaining to medical images is continuously growing as a result of technological advancements in the areas of biomedical imaging equipment and image processing technology. In order to offer telemedicine solutions, these clinical images need to be communicated over a public network between physicians or hospitals. Likewise, due to the restricted computing and storage resources available locally, often the images need to be uploaded to a telemedicine data centre or health cloud. Medical photographs often include private and sensitive information about patients; as a result, the technology that ensures confidentiality and protects patients' right to their own privacy is becoming more vital. The process of transforming data or information from its raw form into a transformed one that conceals the information contained within it is known as encryption. And compression refers to reducing the amount of data included in a graphics file in terms of its size in bytes while maintaining an acceptable degree of picture quality loss. The image data must be shielded against access by unauthorized parties at all costs also shouldn't be unnecessary large. The usage of encryption is what's needed to make the data even more secure. The encrypted image is immune to any type of cryptanalysis that may be performed on it and compression saves the storage space and sped up the transmission process as well. This research presents a literature assessment of several techniques, methodologies, and algorithms for the compression encryption and of medical pictures.

Keywords: Medical Image Encryption, Cryptography, Image security, Decryption.

Introduction

In today's increasingly digital environment, maintaining the privacy of one's personal information is one of the most critical concerns. Smart health care solutions are becoming more popular as a result of recent developments and advancements in the area of computer-assisted diagnostics (CAD). These solutions often rely on artificial intelligence, the analysis of massive amounts of data, and a number of other cutting-edge technologies, all of which help to provide outcomes that are more precise and constrained in time. With the use of the internet, it is now possible to get medical treatment remotely, which may help cure a variety of issues without having to leave the house [1]. The storage and processing for these solutions are often done in the cloud, which enables the data to be disseminated and shared with a variety of domain experts located all over the globe. Additionally, the processing burden may be dispersed among many nodes if necessary. Images obtained from medical procedures are an essential component of the diagnosing process. The majority of the time, various photographs required to be transferred in various parts of the globe to various institutions for diagnosis, such as hospitals, laboratories, or universities. A wide variety of tools may be used for communicative purposes. It is possible to do this task using a variety of portable equipment such as scanners, handheld cameras, and portable x-ray machines, all of which are able to immediately transfer data to a distant server in order to be processed further [2]. One of the prerequisites for providing remote medical care is ensuring the safety of the picture data. The protection of an individual's right to personal privacy is essential. Ethically speaking, it is necessary to protect the patients' right to privacy. The enormous strides that have been made in the field of medicine have resulted in the accumulation of an enormous quantity of data. In order to maintain compatibility with the evolving treatment approaches, it is necessary for this data to be processed and disseminated in an effective manner. During the course of this procedure, you will always face a number of obstacles, the most common of which are insufficient bandwidth and concerns around data safety. The need for both speed and precision is always a challenging goal to work toward achieving. Images that are used for medical purposes are one kind of data that must be compressed while adhering to the requirements outlined and being secure against intrusion [3]. A one-step solution is offered to handle the three problems of lightweight requirements, aggregation needs, and privacy sensitive concerns, and the requirements for devices and sensors that sample medical signals are assessed [4]. According to what has been uncovered in the study, the process of picture compression and encryption may be carried out using any one of the following three methods (also shown in Fig. 1):

1. First, we compress the data, then we encrypt it (CE) in this step, an intruder will have a lower chance of accessing the picture, but encryption may once again result in a larger file size.
2. First, the data is encrypted, then it is compressed (EC) although the size of the picture does not expand throughout this process, an intruder may now have additional hints about how to access it.
3. Compression and Encryption Together or jointly (JCE). This method, which has just lately come into use and may be quicker than the two

methods discussed above, but its operation, is more difficult.

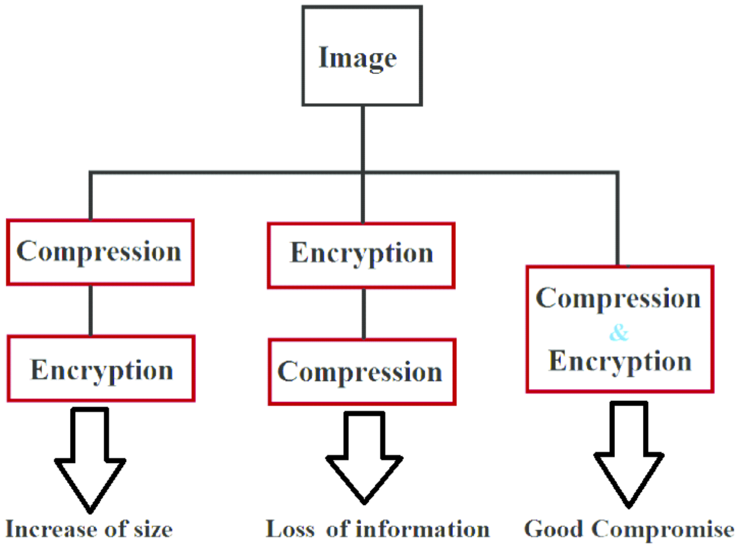

Fig. 1 - Different Image Encryption Approaches

Literature Review

In order to ensure the optimum and safe transmission and storage of medical pictures, Abdmouleh et al. [5] suggested a strategy of partial encryption based on the Discrete Wavelet Transform (DWT) and compatible with the standard JPEG2000 as shown in Fig. 2. This was done in order to protect the privacy of patients. This method is, on the one hand, quicker since it enables a very significant gain in the encryption-decryption processing time (only 6.25 percent of the DWT matrix coefficients will be encoded), and, on the other hand, it is more efficient because it enables the generation of a ciphertext medical image.

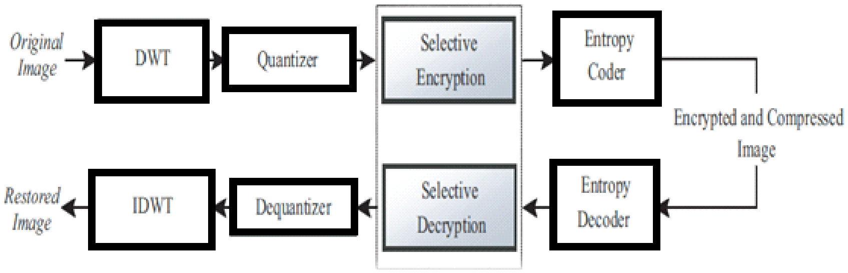

Fig. 2 - Cryptosystem Algorithm [5]

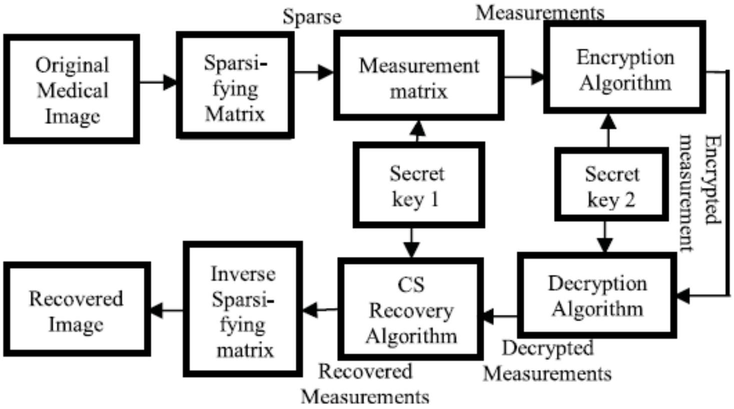

Fig. 3 - Encryption Algorithm [1]

Compressive sensing and chaos driven simultaneous compression-encryption of medical pictures is a concept that was suggested by Ashwini et al. as shown in Fig. 3. In order to begin the process of compressing and encrypting the medical picture I, it is first converted into sparser data by making use of the sparsifying matrix B [1]. The sparser data that was collected is compressively felt with the help of the measurement matrix A, which is built with the help of the suggested chaotic map. This map is produced by combining the sine map with the new logistic map. The Lyapunov exponent and approximation entropy are the two factors that are used in the validation process for comparing the suggested map to the logistic map. Following this step, the collected sensed measurements are encrypted using the suggested encryption technique, and the encrypted measurements are then sent to the receiver. In order to reconstruct the initial medical picture, the receiving end must do the exact opposite of what was described in the preceding section about the compression and encryption technique. On a variety of medical photos, the performance of the suggested approach is evaluated based on a variety of sample ratios.

Chiranjeev et al. [6] suggested a technique for the compression and encryption of medical images that was based on DNA and AES. DNA is a useful medium for the storing of large amounts of data due to its efficiency. Using methods that are based on DNA, this data may be encrypted to protect it from being used maliciously. In this study, we offer a unique compression-encryption technique that is based on DNA and is tailored specifically for use with medical pictures. When broken down into their bit-planes, homogenous pixels make up a significant portion of medical pictures. These pixels become even more apparent when the images are deconstructed. This redundancy may be reduced while compression is taking place, and it was with this idea in mind that the suggested DNA-based Quad Tree Decomposition technique was developed. The full picture is represented by a string of four DNA nucleotides, and the decoding method may be used to reconstruct the picture from these nucleotide sequences into the original picture. The acquired sequences are encrypted with the symmetric key and initial vector parameters using a DNA-based Advanced Encryption Standard (AES) method that is implemented in Cipher Block Chaining (CBC) mode for the purpose of providing security for the sequences that were obtained. The image cannot be recovered from these encrypted sequences unless it is first decrypted using the correct key, and the algorithm for AES is protected against cryptographic attacks. [CDATA] The image cannot be recovered from these encrypted sequences unless it is first decrypted using the correct key.

The chaos-based DNA cryptography was suggested by Prema et al. [7] as a means of enhancing the security of medical pictures. During transmission, the lossless Discrete Haar Wavelet Transform is used to achieve greater efficiency in terms of both space and time. The lossless discrete haar wavelet transform was used to compress the original medical picture, which had a resolution of 512 pixels by 512 pixels. The reconstructed binary picture is then applied to the previously compressed medical image. Each of the sub images I1, I2, I3, and I4 has a dimension of 256 by 256 pixels, and the binary picture has been partitioned into these four sub images. With the use of a 4D Lorenz chaotic map, the chaotic sequences x, y, z, and w were obtained. The erratic sequences x and y are used to scramble the individual pixels that make up the sub images I1 and I2. The pixel values of sub images I3 and I4 are jumbled about after being subjected to the chaotic sequences z and w. In order to generate the one-of-a-kind DNA structure required for each sub picture, the DNA coding rule R1 is applied to sub image I1, whereas rule R3 is applied to sub image I3. In a manner similar to the previous, the DNA coding rule R2 is applied to the sub image I2 while the rule R4 is applied to the sub image I4 in order to produce the one-of-a-kind DNA structure for each sub image. The DNA XOR technique is used to merge the underlying DNA structures of the four sub pictures. The cipher picture may be obtained by using the DNA complementary rules to the process of decoding the combined DNA structure. The cryptanalysis provides conclusive evidence that the suggested cryptosystem is safe from all of the distinct kinds of attacks. Comparisons of the compression ratio and individual pixels are carried out in order to ensure that the preserved medical picture is accurate.

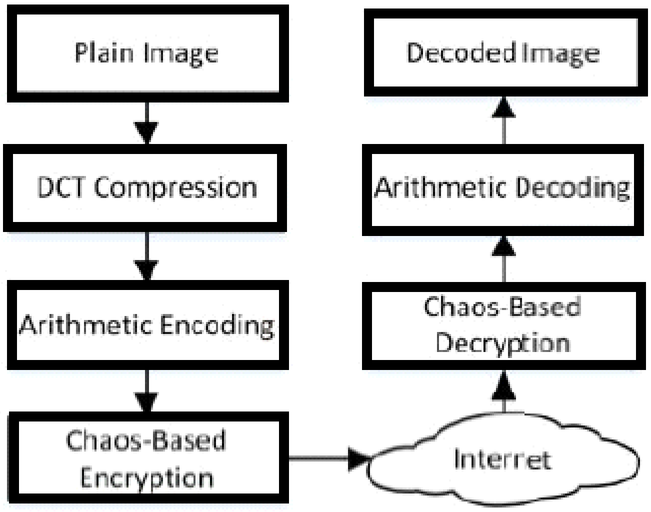

Fig. 4 - Image Encryption Approach [8]

The suggested method by Afandi et al. [8] involves combining the Discrete Cosine Transform (DCT) and Arithmetic Encoding in order to decrease the size of the files containing the medical photos as shown in Fig. 4. The original picture is broken down into its constituent frequencies by the use of the DCT. After that, the frequencies are quantized, which involves reducing or eliminating the frequencies that are not as significant while keeping the frequencies that are significant. The generation of additional zeros is the consequence of deleting the frequencies that are less relevant, which should lead to a reduction in the overall size of the picture file. Following the completion of the DCT-Quantization-IDCT procedure, the picture that was produced is then compressed using the arithmetic encoding method. A sequence input symbol is converted into a floating-point number by the use of arithmetic encoding. The longer and more complicated the information being encoded, the greater the number of bits that are required to meet these objectives. The result of applying arithmetic coding is a number that is larger than or equal to zero and is one less than 1. This is a one-of-a-kind number that can be decoded to yield string symbols that can then be used to make numbers. It is necessary for each symbol to be assigned a set of probability values in order to generate these output numbers. After that, the data that was compressed is jumbled up and made unintelligible by applying two different chaotic sequence functions on it in order to achieve encryption. The suggested method has a compression ratio of 0.748 and a peak-to-average noise ratio (PSNR) of 41.70 dB.

Performance Analysis:

This section depicts some commonly used performance parameters which are used to evaluate the performance characteristics of any image encryption algorithm. Table 1 shows the varying common performance metrics used in different literature.

PSNR: It stands for peak signal to noise ratio. A higher value of PSNR is good because of the superiority of the signal to that of the noise [9].
SSIM: The structural similarity (SSIM) index is a method for measuring the similarity between two images. The resultant SSIM index is a decimal value between -1 and 1[9].
Correlation coefficient: Correlation coefficient (CC) assesses the correlation between two adjoining pixels in an image. It is necessary for the encrypted data to have very low correlation compared to that of original data to avoid statistical attacks [10].
Entropy: The entropy is a quantification of the randomness in gray-levels. The even dissemination of gray-levels indicates that the encryption method is superior [11].

Table 1. Comparison of recent papers based on the evaluation matrices used by them to evaluate performance

References	PSNR	SSIM	CC	Entropy
Abdmouleh et al. [5]	No	No	No	No
Ashwini et al.[1]	Yes	Yes	Yes	No
Chiranjeev et al. [6]	No	No	Yes	No
Prema et al. [7]	No	No	No	Yes
Afandi et al. [8]	Yes	No	No	No

Conclusion

The numerous methods of medical picture compression encryption, as well as the relevant literature, were dissected during the course of this paper. Image security and compression are the utmost important areas in this day and age, particularly when a breach might result in the loss of a human life. In order to validate the recital of the compression encryption methods, a number of different compression encryption strategies are investigated and examined. The original picture is always embedded and encrypted before being sent to the receiver, regardless of the method used and compressed before, after or at the same time. The algorithms, methods, and techniques that were used are all one of a kind. Every day newest encryption compression technology is emerging. The need for more secure encryption methods with a high rate of security will remain till the end of time. The medical picture should be more reliably protected and have a lower overall level of background noise and adequate level of loss of data in order to have the faithful compression.

References

[1]. K. Ashwini, R. Amutha, R. R. Immaculate, and P. Anusha, “Compressive sensing based medical image compression and encryption using proposed 1-D chaotic map,” in 2019 International Conference on Wireless Communications, Signal Processing and Networking, WiSPNET 2019, 2019, doi: 10.1109/WiSPNET45539.2019.9032844.

[2]. A. Sahay, C. Pradhan, and A. Sinha, “Medical signal security enhancement using chaotic map and watermarking technique,” in Handbook of Research on Information Security in Biomedical Signal Processing, 2018.

[3]. E. Setyaningsih, R. Wardoyo, and A. K. Sari, “New Compression? Encryption Algorithm Using Chaos-Based Dynamic Session Key,” Int. J. Smart Sens. Intell. Syst., vol. 11, no. 1, 2018, doi: 10.21307/IJSSIS-2018-004.

[4]. J. Li et al., “A partial encryption algorithm for medical images based on quick response code and reversible data hiding technology,” BMC Med. Inform. Decis. Mak., vol. 20, 2020, doi: 10.1186/s12911-020-01328-2.

[5]. M. K. Abdmouleh, A. Khalfallah, and M. S. Bouhlel, “A novel selective encryption DWT-based algorithm for medical images,” in Proceedings - 2017 14th International Conference on Computer Graphics, Imaging and Visualization, CGiV 2017, 2018, doi: 10.1109/CGiV.2017.10.

[6]. C. Bhaya, M. S. Obaidat, A. K. Pal, and S. H. Islam, “Encrypted Medical Image Storage in DNA Domain,” in IEEE International Conference on Communications, 2021, doi: 10.1109/ICC42927.2021.9500718.

[7]. P. T. Akkasaligar and S. Biradar, “Medical Image Compression and Encryption using Chaos based DNA Cryptography,” in Proceedings of B-HTC 2020 - 1st IEEE Bangalore Humanitarian Technology Conference, 2020, doi: 10.1109/B-HTC50970.2020.9297928.

[8]. T. M. K. Afandi, D. H. Fandiantoro, Endroyono, and I. Ketut Eddy Purnama, “Medical Images Compression and Encryption using DCT, Arithmetic Encoding and Chaos-Based Encryption,” in Proceedings - 2021 International Seminar on Intelligent Technology and Its

Application: Intelligent Systems for the New Normal Era, ISITIA 2021, 2021, doi: 10.1109/ISITIA52817.2021.9502246.

[9]. N. A. Abbas, “Image encryption based on Independent Component Analysis and Arnold’s Cat Map,” Egypt. Informatics J., vol. 17, no. 1, 2016, doi: 10.1016/j.eij.2015.10.001.

[10]. S. S. Askar, A. A. Karawia, and A. Alshamrani, “Image encryption algorithm based on chaotic economic model,” Math. Probl. Eng., vol. 2015, 2015, doi: 10.1155/2015/341729.

[11]. I. S. Sam, P. Devaraj, and R. S. Bhuvaneswaran, “Chaos based image encryption scheme based on enhanced logistic map,” in Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 2011, vol. 6536 LNCS, doi: 10.1007/978-3-642-19056-8_22.