IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Medical Image Encryption Techniques: A Review

Soniya Sarathe[1], Prof. Chetan Gupta[2], Dr. Ritu Shrivastava[3]
M. Tech. Scholar, Department of CSE, SIRTS, Bhopal, India[1], Assistant Professor, Department of CSE, SIRT, Bhopal, India[2], Associate Professor, Department of CSE, SIRT, Bhopal, India[3]

Abstract

Images of patients are often regarded as some of the most crucial and confidential information stored in computer systems. A powerful encryption scheme that is resistant to cryptographic threats is required in order to send medical pictures across a network. Secrecy is the most essential part that needs to be taken much care for in order to ensure the safe storage and transmission of medical images. The protection of users' privacy is the most crucial aspect of information system security, ranking first among the three goals of protection—the others being integrity and availability. This work offers an evident scenario for several current encryption systems for medical photos and gives the results of a comparative study on the encryption of medical photographs. This also encompasses the process of analyzing the requirements for medical photo encryption as well as the level of safety that it offers. The researchers might use this poll to compare the various encryption schemes that have been used up to this point.

Keywords: Medical Image, Encryption, Information Security, DNA, Chaos.

I. INTRODUCTION

Because of advancements in computer network technology, exchanging information between users of personal computers is now becoming much less time consuming and more comfortable. Meanwhile, it provides opportunity for hackers to launch attacks on the network. As a result, the problem of communication security has become more significant in the context of multimedia communications. Image data, including medical photos, photographs from the military, images from electronic publication, and fingerprint images from identification systems, need to be kept private and secret at all times. The current healthcare business relies heavily on the practice of medical image analysis, which in turn has a significant influence on the modern world [1]. When it comes to the diagnosis of biological imaging, automated computer-aided systems are quite helpful since they are quick, accurate, and efficient.

Through the use of remote healthcare systems, both patients and medical professionals are able to execute their duties from their respective places[2]. In addition, within a certain length of time, a physician in a different nation or in any other remote place may be contacted to provide an expert opinion about a patient who is being treated by that physician. It is necessary for digital biological pictures to be sent via a network in order for remote healthcare systems to function [3]. However, the transmission of the biological pictures is coupled with a number of potential vulnerabilities in terms of security. It is essential that the photos be protected from any kind of unwanted access in order to maintain the patients' rightto privacy. In addition, the information included within the biological pictures has to be effectively kept so that it cannot be altered in any way. The manipulation of data may, in many circumstances, have devastating effects. As a result, the procedures and algorithms affecting medical data security are of the utmost significance, and they are among the topics that are receiving the most attention from researchers all over the globe.

Encryption is often used on medical photographs to secure the sensitive information contained within them. The protection of textual data often makes use of standard encryption algorithms and protocols, such as Advanced Encryption Standard (AES), Data Encryption Standard (DES), International Data Encryption Algorithm, and Triple DES. The pixels in medical picture data aren't distributed evenly, there are clear distinctions between regions, and the resolution is quite high. Because they are inefficient when applied to large amounts of data, traditional encryption techniques are not appropriate for the task of safeguarding Digital Imaging and Communications in Medicine (DICOM) pictures. Because of the notable characteristics that chaotic maps possess, including very high ergodicity, unpredictability, and sensitivity to beginning values [4], these maps have found widespread use in a variety of medical imaging cryptosystems. Numerous chaotic encryption algorithms and a variety of enhanced ways have previously been presented; some of the most notable work in this area is shown in next section.

II. LITERATURE SURVEY

Cao et al. [5] introduced an encryption technique that makes use of edge maps that are produced from a source picture. This approach is shown in Figure 2. The method is made up of three different components: a bit-plane decomposer, a generator of random sequence, and a permutation step. Users have access to a variety of options, including the following: Any kind of picture may be utilized as the source image; various edge detectors and thresholds can produce a variety of edge maps; selecting the suitable technique for bit-plane decomposition is adjustable; and the suggested algorithm can be cascaded with a large number of permutation methods. The technique that has been presented to safeguard various kinds of medical pictures has both a key space that is very vast and a key sensitivity that is high.

A method for safeguarding the essential parts of medical images was created by Li et al. [6]. First, the coefficient of variation is used to locate important sections of the picture, also known as lesion areas; next, additional regions are processed as blocks, and the complexity of the texture is examined. The next step in our innovative and reversible data- hiding approach is to embed the contents of the lesion region into a high-texture area. Following this step, an Arnold transformation is used in order to safeguard the initial information about the lesion. After this, a rapid response (QR) code is generated with the help of picture basic information cipher text and decryption parameters. This QR code is utilized in lieu of the original key regions.

The approach that was provided by Li et al. [7] is predicated on a chaotic system that is made up of the two-dimensional Sine Logistic modulation map (2D-SLMM) and the two-dimensional Henon-Sine map (2D-HSM). Zigzag scan scramble, pixel grey value transformation, and dynamic diffusion are the three components that make up the primary encryption technique. A password feedback is added at the step that involves the change of pixel grey value. Because of this, the connection between the password and the key is made more difficult. The suggested method for the encryption and decryption of medical images does not result in any data loss. It sidesteps the issues that arise with low-dimensional chaotic maps, such as those with a tight interval and a small number of parameters, in addition to the issue that arises with the distinctive texture and contour of medical pictures.

Encryption Based on Binary Image Affine Transformation and Zigzag Process was a concept that was developed by Telem et al. [8], illustrated in Fig. 4. Both an external secret key that is 128 bits long and an internal secret key are used in its operation. The techniques that are utilized to extract an internal key in order to apply the zigzag process, the affine transformation, and the substitution-diffusion process are what are considered to be the innovations of the suggested encryption process. At the outset, grayscale pictures are transformed into binary ones from the original image. Binary pictures are parsed in order to get an internal secret key. When combined, the two keys constitute what are known as the substitution diffusion keys. At first, the zigzag technique is performed on each binary picture. Every zigzag binary picture is mirrored or rotated, and then a new grayscale image is rebuilt using an external key. A substitution-diffusion process is carried out by dividing the new picture into a large number of subblocks that do not overlap one another, and each of these subblocks utilizes its own key to do so. We evaluated our algorithms on a wide variety of photos, both biomedical and nonmedical.

Kumari et al. proposed Medical Image Encryption technique based on DNA and chaotic map [9]. There are three steps to this method. 1) The chaotic map produces transformations to shuffles the Image Gray values to achieve high pixel randomness 2) The rules for DNA complementation are generated for perplexing hackers 3) Image grey values are replaced by unique values of DNA sequences and these values are used to generate a random distribution of pixels in an image. Because of the high level of confusion, random distribution properties, and chaotic technique randomness, the proposed technique provides adequate security and cost-effective time for computation.

In this study, a technique that makes use of SHA-256, DNA (deoxyribonucleic acid) cryptography, and a chaotic map is suggested. The approach was supplied by Akkasaligar et al. [10]. It is very crucial to maintain the integrity of the digital medical picture since even the smallest adjustment might result in a significant issue. It is very hard to arrive at an accurate diagnosis of a disease using marginally altered digital medical images. As a result, the concept of integrity becomes the primary focus of this work. The hash key is originally concealed in the digitalized medical image's Least Significant Byte (LSB) after being produced using SHA-256 and buried there for purposes of maintaining the image's integrity. In order to safeguard the picture, it has been encoded using the DNA coding principles. Using Chen's hyper chaotic map, the pixels that make up the encoded DNA matrix are mixed up and dispersed.

Shankar et al.[11] presented their work for the security of medical images. To mitigate the drawbacks of chaos work, the optimal keys were chosen at random. Defined variables and the initial value were used as encryption keys in chaotic cryptosystems. The chaotic maps are designed to be both economical in terms of computational cost and fast. The AGO algorithm was used to define the key. The study also considers the suitability of the encrypted images as PSNR and Correlation Coefficient values for optimization. The benefits of massive key-space and high-level security while maintaining efficiency at satisfactory levels. As a result, one level of encryption using the AGO algorithm is sufficient to defend against different attacks.

Shalaby et al. [12] proposed arnold chaotic AES-based medical image encryption. In the beginning, they used a Butterworth High Pass Filter to make sure that medical information wouldn't be lost during the encryption process. The proposed method is then modified by combining Arnold chaos technique with the widely used AES algorithm. Three bits are framed and introduced to the standard AES key by modifying Arnold's cat map technique, improving the overall encryption robustness. The proposed encryption technique is compared to current literatures. The comparative study demonstrates that the method is able to improve both the strength of the cryptographic process and the quality of medical images while lowering overall computational cost.

Han et al. [13] proposed medical image encryption algorithm based on Hermite chaotic neural network. The logistic map is used to generate chaotic sequences that are then used in the medical image encryption algorithm. Second, a Hermite chaotic neural network is trained using this chaotic sequence. Two

keystreams are then used to encrypt the medical image using the trained Hermite chaotic neural network. The effectiveness of the encryption algorithm has been demonstrated experimentally. The security analysis demonstrates that the encryption algorithm significantly enhances the security of medical images, as it is resistant to statistical analysis, has strong key sensitivity, a large keyspace, and greatly improves image quality.

The algorithm presented by Choi et al. [14] involves both phased replacement and phased rearranging. In the algorithm, 1D programmable Cellular atomata (PCA) with two complement vectors is used to generate the key stream during the image's substitution phase. In addition, the key stream is used to alter the original image's pixel values before the Chen chaotic system is applied. In this stage, 1D PCA generates a nonlinear key stream with a longer period and higher efficiency than existing MLCA, and the Chen chaotic system is used to strengthen the security of the proposed algorithm. To speed up the encryption process, they shuffle the position of each pixel in the image using 1D MLCA during the shuffling phase. While 1D MLCA is faster than modified 3D chaotic cat maps, it is also more chaotic than standard chaotic maps. This cryptosystem's security has been improved by a number of factors, including its CC, NPCR, UACI, key space, resistance to data loss and noise attacks, and so on.

Sarosh et al.[15] presented a rapid chaos-based medical image cryptographic algorithm. For ambiguity and diffusion, the scheme employs a multiple chaotic map like Logistic, Chebyshev, and Piecewise. The image is first circularly shifted, and then bit plane slicing is performed. The plane formed by the XOR operation between the MSB and 7th ISB plane replaces the Most Significant Bit (MSB) plane. The resulting image is scrambled using the Logistic map's Pseudo Random Number. To determine the initial condition for the Piecewise logistic map, the scheme is adaptive and calculates image parameters such as sum or mean. The piecewise map is used to produce a key image, which is then XOR with the shuffled image. At the end, a Chebyshev map iterates and a random sequence is generated to permute the image pixels and produce ciphered image. The cryptosystem has been tested on a variety of medical image types and sizes, as well as natural images.

Goje et al. [16] proposed a medical image encryption algorithm based on a double chaotic map. In the algorithm, permutation is represented by a 2D chaotic map, while diffusion is represented by a 3D chaotic map. The concepts of confusion and diffusion are heavily used in encryption methods. A color transformation is used to convert the RGB color system to the YCbCr color space. After that, a block permutation will be used to rearrange the order of the 16 blocks that make up each of these parts. A pixel permutation technique is also used to increase confusion. Because permutation alone is insufficient to achieve satisfactory encryption, the contents were subjected to diffusion once more to obtain the final cipher text image. To evaluate the safety of the proposed system, researchers conducted experiments and analyzed the results using a variety of metrics, including histogram analysis, correlation, NPCR, UACI, entropy, etc.

III. PROBLEM DOMAIN

After reviewing the literature, we identify the following issues and areas with the methods under consideration:

1. Since most chaotic encryption methods rely on floating-point computations, it is difficult and time-consuming to implement them practically in software or hardware, especially when compared to more conventional cryptosystems like AES and DES. Traditional image encryption methods have various drawbacks, including data padding waste, difficulty to decode, inability to recognize images without decoding, and exposing of private information after decryption.

2. DNA encryption is chosen by information security researchers preferably because of DNA's nucleotide sequence's vast storage capacity, high parallelism, and low energy consumption.

References	NPCR & UACI	Correlation Coefficient	SSIM	Entropy	Histogram analysis
Cao et al. [5]	0.9960, 0.3348	-0.0074,0.0019,-0.0017	-	-	-
Li et al. [6]	-	-	0.8267	-	Passed
Li et al. [7]	98.7677,32.8412	−0.0009,−0.0017,0.0006	-	7.9998	Passed
Telem et al. [8]	99.6159,33.5402	−2.57e−03,−3.56e−03,−2.56e−04	-	7.9992	Passed
Akkasaligar et al. [10]	99.77, 33.23	(0.992)	-	7.76	-
Goje et al. [16]	99.32, 31.6478	-0.0006201, 0.00064, -0.000328	-	7.9972	Passed
Shalaby et al. [12]	99.23740, 33.93210	0.00046	-	-	-
Han et al. [13]	-	-	-	-	Passed
Choi et al. [14]	99.619, 33.364	-0.0030, 0.0040, 0.0044	-	-	-

The following are some common metrics used to assess the efficacy of an image encryption algorithm. The most widely-used performance indicators are shown in Table 1 below. Common metrics for evaluating the resistance of image encryption algorithms to differential attacks include the unified averaged changed intensity (UACI) and the number of changing pixels per second (NPCR) [17] [18]. You can determine how similar two images are by using a measure called the structural similarity (SSIM) index. The resulting SSIM index takes a decimal value between -1 and 1 [19]. Similarity between two neighboring pixels in an image is quantified by the correlation coefficient (CC) [20] [21]. The encrypted data must have a very low correlation with the original data in order to prevent statistical attacks. The entropy of a gray scale image is a quantitative representation of the image's inherent randomness. As evidenced by the relatively even distribution of gray scale values, the encryption technique appears to be robust. A histogram, a two-dimensional graph displaying the distribution of gray scales according to their attributes, is present in digital images. As a result, the main contribution of this article is to provide a brief overview of medical image encryption, as well as background information and evaluation metrics. We then provide a thorough examination of various medical image encryption schemes, as well as their advantages and disadvantages. In addition, the contribution of the surveyed scheme is summarized and compared in light of the estimation evaluation parameters.

IV. Conclusion and Future Work

Medical image security is needed not only to preserve confidentiality and handle confidentiality concerns, but also to prevent approved and illegitimate users from modifying the pictures. Thus, all data, especially medical photos, may be secured. Medical image encryption guarantees data and image confidentiality. In this study, we reviewed medical picture encryption approaches and related information. Different articles have offered spatial and frequency domain techniques. Medical treatment demands high-quality photos with no modifications. Medical image encryption must withstand network attacks.

From the above literature review it is concluded that distinct authors have used different parameters for the evaluation of the encryption algorithm. It is also inferred that correlation coefficient is the important parameter of the evaluation as for as the image encryption is concerned. Based on the above study we provide the following future directions which can be helpful:

1) One should use Powerful encryption technique which does not burden the system.
2) One should use the method that has vast storage capacity, high parallelism, and low energy consumption.
3) Hybrid combination of two methods better than one method because it can contain more number of features that can increase the security.
4) The transform domain methods like Fourier Transform, Cosine Transform and Affine Transform etc. with powerful encryption technique like DNA can satisfy the above mentioned points.

References

[1] R. K. Sinha, N. San, B. Asha, S. Prasad, and S. S. Sahu, ―Chaotic Image Encryption Scheme Based on Modified Arnold Cat Map and Henon Map,‖ in Proceedings of the 2018 International Conference on Current Trends towards Converging Technologies, ICCTCT 2018, 2018, doi: 10.1109/ICCTCT.2018.8551137.

[2] M. Tayachi, S. Mulhem, W. Adi, L. Nana, A. Pascu, and F. Benzarti, ―Tamper and clone-resistant authentication scheme for medical image systems,‖ Cryptography, vol. 4, no. 3, 2020, doi: 10.3390/cryptography4030019.

[3] P. Sreenivasulu and S. Varadharajan, ―Algorithmic Analysis on Medical Image Compression Using Improved Rider Optimization Algorithm,‖ in Lecture Notes in Networks and Systems, vol. 103, 2020.

[4] 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.

[5] W. Cao, Y. Zhou, C. L. P. Chen, and L. Xia, ―Medical image encryption using edge maps,‖ Signal Processing, vol. 132, pp. 96–109, 2017, doi: 10.1016/j.sigpro.2016.10.003.

[6] 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.

[7] S. Li, L. Zhao, and N. Yang, ―Medical Image Encryption Based on 2D Zigzag Confusion and Dynamic Diffusion, Secur. Commun. Networks, vol. 2021, 2021, doi: 10.1155/2021/6624809.

[8] A. N. Kengnou Telem, C. Feudjio, B. Ramakrishnan, H. B. Fotsin, and K. Rajagopal, ―A Simple Image Encryption Based on Binary Image Affine Transformation and Zigzag Process,‖ Complexity, vol. 2022, 2022, doi: 10.1155/2022/3865820.

[9] K. S. Kumari and C. Nagaraju, ―DNA encrypting rules with chaotic maps for medical image encryption,‖ in Proceedings - 5th International Conference on Intelligent Computing and Control Systems, ICICCS 2021, 2021, doi: 10.1109/ICICCS51141.2021.9432176.

[10] P. T. Akkasaligar and S. Biradar, ―Medical Image Encryption with Integrity Using DNA and Chaotic Map,‖ in

[11] Communications in Computer and Information Science, 2019, vol. 1036, doi: 10.1007/978-981-13-9184-2_13.

[12] K. Shankar, M. Elhoseny, E. D. Chelvi, S. K. Lakshmanaprabu, and W. Wu, ―An efficient optimal key based chaos function for medical image security,‖ IEEE Access, vol. 6, 2018, doi: 10.1109/ACCESS.2018.2874026.

[13] M. A. W. Shalaby, M. T. Saleh, and H. N. Elmahdy, ―Enhanced Arnold's Cat Map-AES Encryption Technique for Medical Images,‖ in 2nd Novel Intelligent and Leading Emerging Sciences Conference, NILES 2020, 2020, doi: 10.1109/NILES50944.2020.9257876.

[14] B. Han, Y. Jia, G. Huang, and L. Cai, ―A Medical Image Encryption Algorithm Based on Hermite Chaotic Neural Network,‖ in Proceedings of 2020 IEEE 4th Information Technology, Networking, Electronic and Automation Control Conference, ITNEC 2020, 2020, doi: 10.1109/ITNEC48623.2020.9085079.

U. S. Choi, S. J. Cho, and S. W. Kang, ―Color Image Encryption Algorithm for Medical Image by Mixing Chaotic