JOURNAL OF BASIC SCIENCE AND ENGINEERING

"SECURING TELERADIOLOGY: A COMPREHENSIVE REVIEW OF TECHNIQUES AND CHALLENGES"

Nikhila S[1] and Dr. Krushnasamy V S [2]
DayanandaSagar College of Engineering, Bangalore, India
nikhilamsrit@gmail.com[1]and krushnasamy-inmt@dayanandasagar.edu[2]

ABSTRACT

One area of telemedicine is teleradiology, which is the transfer of radiological images, such as MRIs, CT scans, and X-rays, from one place to another for interpretation or consultation. Technological developments have given this sector more significance, especially in the areas of medical imaging and communication. Considering the private and sensitive nature of medical images, such as X-rays, MRIs, CT scans, and other diagnostic images, medical image security is a vital component of healthcare IT. In order to uphold patient privacy, adhere to legal requirements, and stop unwanted access or alteration, these images must be protected. In this paper, we propose a literature review of techniques in teleradiology and their challenges. The latest existing works are reviewed, their limitations are analyzed, and the future scope of their implementation challenges is addressed.

INTRODUCTION

Medical authentication refers to the processes and technology used in the healthcare business to certify the identification of individuals seeking access to medical information, systems, or facilities. The purpose is to ensure that only authorized individuals have access to sensitive health data, thereby protecting patient privacy and complying with healthcare requirements.Maintaining patient information's availability, confidentiality, and integrity as well as the general security of healthcare systems requires effective medical authentication. The healthcare sector keeps looking at and using new authentication techniques to improve security and safeguard patient data as technology develops.

The medical image is considered an essential element in the discipline of telemedicine. For diagnostic purposes, hospitals employ it. Thus, the doctor's diagnosis will be affected by any alteration, no matter how minor. To make sure that only real alterations take place, medical images require extreme security. These days, transmitting medical images between clinics in several states is a very common practice. Unfortunately, because this transaction takes place over

open, insecure networks, there is a chance that malicious actors may intervene, which could lead to altered or erased data. Owing to these variables and dangers, telemedicine needs to provide secure exchange conditions to guarantee the authenticity and integrity of medical images while they are being transmitted.

Various medical pictures are taken in hospitals and stored in databases for use during research and diagnosis. These databases need to be protected from both accidental and deliberate intrusions. These kinds of databases enable early illness diagnosis and treatment possible. Meanwhile, the doctor needs to make sure the image is free of modifications before reaching a decision.

In order to maintain secrecy, only authorized users are allowed to examine and alter the medical image; unauthorized users are not permitted to do so or to extract any information from it. The encrypted medical image [1] can be decrypted and the patient data accessed by the user who has the key on the destination side. To ensure this, cryptography is essential. For a medical image to be considered authentic, it must match the one that was sent from the source exactly and be associated with a specific patient when it arrives at its destination.

The final factor to evaluate is reliability. It is in charge of preserving the system's availability and integrity. "Integrity" describes the requirement that the medical image that is received remain unaltered. Another way to do this is to take the watermark out of the received image and extract it exactly where it is. "Availability" is having a medical image available when a doctor or other medical party requests it. The destination and source are the same and are related to a certain patient. Using cryptographic techniques, the data is protected during the transition. By knowing the secret key and algorithm, someone can decrypt the data and put it in a format that can be used. Decryption, however, renders the data insecure. It is therefore quite challenging to ascertain its origin and authenticity. This kind of security is known as priori protection measures. As extra safeguards against data integrity, validity, and originality, watermarking techniques were created. After decryption, we can still determine if the data has been altered or is in its original state.

Securing and demonstrating the security of medical photographs is one of our study's objectives. This means demonstrating the originality, integrity, and authenticity of the medical image

(owner). Ultimately, this research aims to support the healthcare system in creating a robust, safe, and private system for the interchange and utilization of medical pictures.

1.1 Medical Image Encryption Techniques

Some of the encryption techniques used are:

1. Water Marking

The technique of hiding a medical image in a carrier signal is called watermarking [2]. The medical image doesn't have to be linked to the carrier signal in order to function. The validity and integrity of the medical image can be verified using these digital watermarks. The scenarios in which digital watermarking is employed largely dictate the qualities that are necessary. In order to ensure anonymity, a more robust watermarking technique must be employed, and the digitally watermarked images must be resistant to alteration during transmission

2. Cryptography

The cryptography technique [3] establishes the security issues by assuming that the sender and recipient are intended parties and possess keys, which are security features. Consequently, the individual holding the key (the recipient) can decode and view the content of the digital information once the sender has encrypted it.The cryptography method determines the security issue by supposing that the intended sender and recipient possess keys, which are security features. These keys can be distinct (asymmetric), which means that the key used on the sender side differs from the key used on the receiver side, or they can be the same (symmetric) on both sides. The algorithm used in symmetric encryption is called a cypher. Encryption techniques fall into one of two categories: block or stream cyphers, depending on how data is handled. Security concerns including secrecy, authenticity, and dependability are also guaranteed by cryptography. The data is accessible to the user, the user is authorized to read the data, and the user is not authorized to access the data.Symmetric, asymmetric, and hash function cryptographic techniques are the three main categories. They are all dependent on a group of elements called keys. Symmetric encryption uses a single key called the private key for both encryption and decryption. Two keys are utilized in asymmetric encryption: the public key is used for

encryption, and the private key is used for decryption. Symmetric encryptions come in two varieties: block cypher and stream cypher.

3. Techniques for Hybrid Watermarking and Cryptography

The data is safeguarded by cryptographic methods throughout the transfer. With the secret key and algorithm, someone can decrypt the data into a format that can be used. But after the data is encrypted, it becomes very challenging to verify its authenticity and integrity. This kind of protection is known as priori protective measures. In addition to other data security measures, watermarking techniques were created to prove data availability, validity, integrity, and uniqueness, among other things. After decryption, we can still decide if the data has been altered or is in its original state. Divided into two methods:

i. Encryption is followed by watermarking (WFE)

This method involves inserting the watermark into the host data and then encrypting the watermarked data. On the recipient's end, the watermarked encrypted data is decrypted before the watermarked data is extracted.

ii. After encryption, there is watermarking (EFW)

In this technology, the encrypted watermark is integrated into the encrypted original data. Bonus: homomorphism encryption is provided. This will take place in the field of cryptography. On the other hand, before decrypting the encrypted original data and watermark, the decoder needs to extract them.

1.2 Properties of Encryption Techniques

Some of important properties are

i. Robustness

The robustness of the watermark is its ability to resist many kinds of attacks. Attacks using image processing techniques like noise, cropping, and geometric alterations—such scale and rotation—occur often. The strikes could be focused assaults meant to eliminate and destroy the target. Unintentional attacks on the watermarked image, or the addition of a watermark to the image while it is being transmitted with the goal of erasing or deteriorating the watermark.

ii. Imperceptibility

Imperceptibility is the quality loss that occurs between the original and watermarked images. Most of the time, the watermarked image ought to be perceptually identical to the original. This characteristic is known as the watermarking approach's transparency or imperceptibility. The entire procedure is ineffective if the original image after embedding is damaged during the watermarking process. Some applications, such a channel logo, a person's name on an item, or other applications that want to display who owns the materials, may have low imperceptibility because they want the watermark to be visible to human eyes. To assess the imperceptibility components of the watermarking system, we calculate the fidelity between the watermarked and original images.

iii. Security

A watermarking system is deemed secure if it is resistant to deliberate manipulation attempts. It would offer great security, even if the attacker knew how to implant and extract the watermark. Based on the key, the watermark's security strength is selected. Think about the following circumstance: If the key used to unlock the system is secure, the hacker can attack the watermark and try to implant a fake one by removing it from the watermarked image. The system will reject the hacker. Robustness and security are not the same thing.

iv. Computational Complexity

One crucial and significant issue is the watermarking system's computational complexity. Both the size of the original image and the watermarked image define the watermarking system's capacity. The capacity is indirectly impacted by the computational complexity.In contrast, the second most important factor in the complexity equation is time. The temporal complexity can be determined by the algorithm's speed. To have minimal time complexity, the embedding and extraction processes have to be fast.

2. LITERATURE SURVEY

AkramBelaziet al.,[3] have introduced a novel medical image encryption method that utilizes DNA encoding and chaos [4]. In the case of two encryption rounds, the suggested approach

combines chaos and DNA calculations, with the key generation level leading the way and the permutation-substitution-diffusion structure coming next. Experiments have demonstrated the suggested technique's resistance to all types of attacks. Given its great potential for secure and real-time imaging applications, the suggested technique's minimal complexity makes sense.Saleh Ibrahim et al., have presented a framework for effective medical image encryption using dynamic S-boxes and chaotic maps [5]. The suggested method employs an S-box substitution approach before and after the chaotic replacement, which has been shown to successfully withstand attacks using selected plaintext and selected ciphertext. Experiments indicate that, irrespective of the chaotic map employed for execution, the suggested architecture satisfactorily endorsed every security test.

Tahir Sajjad Ali and Sashid Ali have presented a novel medical image signcryption scheme using TLTS and the Henon Chaotic Map [6]. The technique for encrypting medical photos that guarantees the privacy of private medical information during transmission is covered in this study. The suggested approach is approved by the mixed strategy of hybrid cryptography. Trials indicate that the proposed technique offers non-repudiation, confidentiality, authenticity, and integrity.

A fast-reaching finite-time synchronization solution for chaotic systems was created by BehrouzVaseghi et al., [7] and may find application in the encryption of medical images. In this research, the authors first developed a tracking approach for adaptive terminal sliding modes with fast reaching conditions. They then developed a chaotic cryptosystem that uses a synchronized chaotic scheme as the secret key generator. The results of the experiments demonstrate the high rate of convergence, ease of use, and dependability of the suggested technique.The following individuals have presented a lightweight encryption technique to improve medical image security on the Internet of Medical Things: Md. Arif Hassan, Shayla Islam, RossilawatiSulaiman, and Muhammad KamrulHasan [8]. This study examines how an effective, lightweight encryption algorithm might improve a safe picture encryption strategy for the healthcare industry. The suggested lightweight encryption method makes use of two permutation techniques to safeguard medical photos. Trials indicate that the proposed method is more efficient than conventional procedures in terms of time for medical photos.

Yi Ding, Fuyuan Tan, Zhen Qin, and Mingsheng Cao suggested DeepKeyGen: A Deep Learning-Based Stream Cipher Generator for Medical Image Encryption and Decryption [9]. The learning network is considered to be the adversarial network (GAN) in DeepKeyGen in order to create the private key. In the meantime, the area of modification has advanced to the point where it is able to keep an eye on the learning network and gather data regarding the generation of private keys. Trials show that the suggested method encrypts multimodality medical pictures successfully and with good performance.

The authors Un Sook Choi, Sung Jin Cho, and Sung Won Kang [10] proposed combining NCA with the 3D Chaotic Cat Map to encrypt color medical pictures. The NCA is a pseudo-random number generator (PRNG) made out of one extreme length cellular automata and two non-linear cellular automata. It is non-linear and expands keyspace. The new color medical photo encryption method has proven to be extremely safe and dependable in tests.YuanyuanJia, Guo Huang, LishaCai, and Baoru Han also offered proposals [11]. A Chaotic Neural Network-Based Hermite Method for Encrypting Medical Images The proposed technique's medical picture encryption algorithm first creates a chaotic sequence using the logistic map. After training a Hermit chaotic neural network with the chaotic sequence, two key streams are employed to encrypt the medical image. Strong key compassion, statistical analysis confrontation, and good encryption and decryption effects are all demonstrated by the suggested approach.

Sahar Haddad, GouenouCoatrieux, Alexandre Moreau-Gaudry, and Michel Cozic propose Joint Watermarking-Encryption-JPEG-LS for Medical Image Reliability Control in Encrypted and Compressed Domains [12]. The key advantage of the proposed technique is that it has been positively welcomed for its capacity to allow access to security features based on watermarking from bit streams of compressed and encrypted images without requiring even a minimal amount of decryption. Experiments on the proposed method show that it minimizes image distortion and transfers a message in both encrypted and compressed fields with high reliability.Sara T. Kamal, Khalid M. Hosny, and Mostafa M. Fouda [13] have proposed a new method for encrypting medical pictures in both grayscale and color. This study offers a brand-new image block-based picture enhancement technique. After that, the image blocks are joined using a permutation, rotation, and random pattern. A confused logistic map is then used as a clue to decipher the

jumbled image. Experiments have shown that the suggested method can successfully encrypt medical pictures in both color and grayscale.

In smart healthcare IoT systems, Jalaluddin Khan, Jianping Li, Amin UlHaq, ShadmaParveen, and Sana Ullah proposed medical picture encryption [14]. The purpose of this effort is to secure medical data via image encryption. The authors employ pixel adaptive dispersion theory in conjunction with three rounds of high-speed knotting to remove casual neighboring pixels. The suggested method for safeguarding the smart healthcare IoT system has a high security level, per the trial results.Yi Ding, Guozheng Wu, Dajiang Chen, and Ning Zhang suggested DeepEDN: A Deep Learning-based Image Encryption and Decryption Network for the Internet of Medical Things [15]. More precisely, the medical picture is moved from its original field to the targeted field using the cycle-generative adversarial network (Cycle-GAN) as the main learning network in DeepEDN. The studies show that the suggested method can more successfully encrypt and decrypt the medical image while maintaining a high-security layer.

Prema T. Akkasaligara and SumangalaBiradar [16] suggested encrypting particular medical photos using DNA cryptography. This article employs dual hyperchaotic map methods and DNA cryptography to bring high-level security to medical imaging. Because digital photographs are larger, processing takes longer. Tests have demonstrated that the suggested approach requires less computation time, which qualifies it for use in telemedicine, smart health, and e-health applications.RichaMaurya, Ashwani Kumar Kannojiya, and Rajitha B. have presented an Extended Visual Cryptography Technique for Medical Image Security [17]. Secret data can be distributed in visual, textual, and other media using visual cryptography. The medical image is first encrypted in the suggested technique and then it is inserted into three cover images. Trials show that the insertion and encryption techniques used in this process are less complex and lossless.

For medical picture encryption, Sumit Kumar, BhaskarPanna, and Rajib Kumar Jha [18] proposed a fractional discrete cosine transform with chaotic function. This work presents a novel approach to medical data protection: the use of a chaotic map on the fractional discrete cosine transform (FrDCT) coefficients of medical images. The two steps of the projected algorithm are the application of FrDCT on the picture and the chaotic map on FrDCT coefficients. The

suggested approach need to have a closer relationship with other cutting-edge techniques based on the results of the experiments.

Priya and B. Santhi [19] proposed a novel visual medical image encryption method for the safe transfer of authenticated watermarked medical photographs. The existence of secret data in an encrypted image is indicated by the use of an anonymous, noise-like image format in basic picture encryption. To address this issue, this study suggests a revolutionary visual medical image encryption technique that secures the existence of watermarked medical images. Experiments have demonstrated that the suggested method reduces the invader's task while achieving a respectable outcome.

Zeesha Mishra and BibhudendraAcharyan [20] presented high throughput and low-area architectures of secure IoT solutions for medical picture encryption. This paper presents low-area, high-speed SIT algorithm architectures for reserve force applications. The projected sequential design is more favorable in low-area situations, whereas the projected pipeline architecture is more useful in high-frequency applications. Experiments on the suggested approach show that it is faster and needs less room, which lowers the cost of hardware.

For medical photo encryption in the dual domain, AashiqBanu S. and RengarajanAmirtharajan [21] proposed a chaos-DNA-IWT combo approach. In this study, DICOM image encryption is recommended. The suggested method makes use of a logistic map and a chaotic 3D Lorenz attractor to create pseudo-random keys for encryption. The outcomes demonstrate how robust to brute force attacks the suggested strategy is.

Xiuli Chai, Jitong Zhang, ZhihuaGan, and Yushu Zhang have proposed a medical picture encryption method based on Latin square and memristive chaotic systems [22]. In the suggested approach, the diffusion and permutation architecture is employed. Using Latin square and plain image data, a permutation-based on Latin square and plain image (PPILS) is proposed. Trials with the project have demonstrated that it has enhanced the robustness and security of picture encryption, which can be used for medical image encryption applications.Joshua C. Dagadu, JianPing Li, and Emelia O. Aboagye suggested Medical Image Encryption Based on Hybrid Chaotic DNA Diffusion [23]. The two stages of the suggested strategy are distributing DNA and generating a chaotic key. The message abstract technique operates row-by-row between the two

chaotic matrices and the plain image matrix after applying five hash functions on a simple medical image. The predicted strategy is dependable and defies several epidemic procedures, according to the results of the numerical, differential, and key analysis trials.

3. INFERENCES

Using a suitable and efficient strategy and methodology is essential when putting the medical photo encryption technology into practice. All of the papers that have been evaluated so far have been assessed using physical metrics. Most of the papers employed measures like PSNR and SSIM, although their computations do not take into consideration all of the features in the image. Expert systems for medical image evaluation must therefore monitor the variations between the original and encrypted images

Following a thorough review of the literature on medical image encryption, the following analysis was used to formulate the problem statement:

Table: Comparative Analysis of Image Steganography Techniques in Medical Imaging

Sr. No	**Authors**	**Technique**	**Publication**	**Limitation/Problem**
1	Ghazanfar et al., [24]	Suggested an improved technique for image steganography to increase the data-hiding ability and imperceptibility of stego images using Image Region decomposition (IRD) technique	*IEEE Access* *2020*	Suited only for specific type of Brain MRI Images
2	Lopez et al.,[25]	An ANN is configured to repeat a secret message from a cover image using the proposed Scale Conjugate Gradient (SCG) learning method.	IEEE LATIN AMERICA TRANSACTIONS, VOL. 18, NO. 3, MARCH 2020	More number of ANN architectures were used increasing training time.
3	J. Tao et al., [26]	Compression strategy with coefficient adjustment to maintain similarity between	*IEEE Trans. Circuits Syst. VideoTechnol.*	Not able to achieve high non-detectability.

		the compressed and original stego images.	*2019*	
4	Li and Zhang et al., [27]	A key method that is built straight from a hidden message to conceal secret data in a fingerprint image	*IEEE Trans. Image Process.* *2019*	Complex processing
5	Elhoseny*et al.*[28]	Patient data can be embedded in any cover media using level 1 and level 2 2D discrete wavelet transform algorithms. RSA and hybrid AES are employed.	*IEEE Access* *2018*	Both AES and RSA increases the complexity.

This table provides an overview of different image steganography techniques in medical imaging, highlighting the authors, techniques, publications, and limitations or problems associated with each approach.

The proposed algorithm by Siddiqui et al. aims to enhance the imperceptibility and data hiding capacity of stego images in medical and e-healthcare systems. The algorithm decomposes grayscale MRI images into three regions and operates on the least significant bits of each pixel to embed secret information. The algorithm achieves better imperceptibility by adjusting thesecond and first least significant bits in the low-intensity region. The performance of the algorithm is evaluated using peak signal-to-noise ratio (PSNR), mean square error (MSE), and structural similarity index (SSIM). The results show that the proposed algorithm provides better average PSNR compared to other method. The algorithm significantly improves imperceptibility and data embedding capacity compared to existing methods.

Stenography, a practice of writing dictations at high speed, is being preserved using Convolutional Neural Networks (CNN) and image processing techniques. This research used 2000 common court stenography words and phrases to train the CNN model, which was enhanced by applying canny edge detection for better classification accuracy. The results showed that machines can now recognize stenography writings through CNN, thanks to the use of canny

edge detection. This study opens up possibilities for the continued use of stenography in modern times.

In addition to these advancements in steganography techniques, researchers have also been exploring the potential of utilizing generative models in deep learning for constructing robust steganography. These generative models enable the development of new frameworks that offer increased flexibility and effectiveness compared to existing approaches. Moreover, experiments have demonstrated that these generative robust steganography frameworks exhibit higher secret information embedding capacity and enhanced steganography image quality when compared to traditional methods this signifies a significant leap forward in the field of steganography, as it opens up possibilities for more adaptable and secure methods of concealing confidential information within multimedia objects.

[27] Construction-based data hiding refers to a technique where secrets are transformed into fingerprint images. This approach aims to enhance the security and robustness of data hiding methods. The proposed method in the paper by Li and Zhang focuses on the construction-based data hiding using secrets and fingerprint images. The authors present a technique that utilizes quick response (QR) codes and polynomial-based secret image sharing (SIS) schemes. The output shadows in their scheme are valid QR codes, making them comprehensible and robust to typical noises. The secret image can be losslessly restored using barcode scanning operation and Lagrange interpolation with any k or more shadows. The proposed scheme reduces suspicion from attackers and improves the management efficiency of shadows, making it applicable to noisy channels

[28]The security of patient information is crucial in IoT-based healthcare systems. The Internet of Medical Things (IoMT) enables the safe exchange of data, but encryption models for IoMT devices are not fully optimized due to limited processing power, memory, and battery life. To tackle this issue, lightweight encryption algorithms have been developed to provide strong security while minimizing computational and power requirements. For example, a study implemented a lightweight-medical image cryptography (LW-MIC) system using ensemble lightweight cryptographic (ELWC) protocols, which improved image encryption and reduced time complexity. Another study introduced a Raspberry Pi cryptosystem for real-time transmission of patient health data, utilizing chaotic maps to generate highly random encryption

keys. These advancements contribute to the secure transmission of medical data in IoT-based healthcare systems.

4. LIMITATIONS

In order to assure the future success and growth of teleradiology while placing a priority on patient care and data security, addressing these issues calls for a combination of technology advancements, governmental actions, and industry collaboration.

- Sensitive medical picture transmission via networks raises questions regarding patient privacy and data security. Although it can be difficult to maintain across several platforms, compliance with healthcare standards, such as the Health Insurance Portability and Accountability Act (HIPAA), is essential.
- Radiologists that work in teleradiology might have to obtain licences from several different authorities, which can be a difficult and drawn-out procedure. Maintaining the standard of interpretation across many locations and making sure radiologists have the right credentials are ongoing challenges.
- Transmission of pictures from various sites with differing equipment and image quality criteria is a common practice in teleradiology. Inconsistent image quality can cause problems for radiologists and affect the precision of diagnoses.
- It may be difficult to give timely interpretations and consultations when teleradiology services are rendered across time zones. Managing workflows efficiently, especially in emergency circumstances, can be problematic when there are large time disparities between the imaging facility and the interpreting radiologist.
- Workflow interruptions may result from difficult and time-consuming integration with current HIS and PACS. The effectiveness of teleradiology services may be impacted by system compatibility problems.

5. CONCLUSION

The necessity for medical image protection is not only to preserve confidentiality and handle confidentiality difficulties, but also to prevent medical images from being modified by both authorized and unauthorized users. As a result, there is a way for maintaining data security, including medical imaging. In medical concepts, medical image encryption is a well-known

method of ensuring data and picture confidentiality. In this study, we offered a comprehensive overview of medical image encryption algorithms and explored a variety of related topics. Medical care necessitates the highest image quality and will not accept any image modifications. As a result, the process of medical picture encryption must be resistant to all types of network attacks.While integrating medical photo encryption into a medical system, it is imperative that we choose a practical method. Physical measures that are commonly used for assessing medical picture encryption, such PSNR, SSIM, and others, were used to assess the effectiveness of all the encryption strategies offered in this study. These measures do not account for every factor required to produce an accurate and clinically appropriate medical image. Therefore, this survey highly advises reviewing the use of clinical needs in order to increase efficiency.

References

[1] Hua, Z., Yi, S., & Zhou, Y. (2018), Medical image encryption using high-speed scrambling and pixel adaptive diffusion, Signal Processing, 144, 134–144. doi:10.1016/j.sigpro.2017.10.004

[2] Lakshmi, C., Thenmozhi, K., Rayappan, J. B. B., &Amirtharajan, R. (2018). Encryption and watermark-treated medical image against hacking disease—An immune convention in spatial and frequency domains. Computer Methods and Programs in Biomedicine, 159, 11–21. doi:10.1016/j.cmpb.2018.02.021

[3] M. T. I. Siyam, K. M. R. Alam, and T. Jami, “An exploitation of visual cryptography to ensure enhanced security in several applications,” Int. Journal of Computer Applications, Vol. 65, No. 6 pp. 42-46, 2013.

[4] AkramBelazi, Muhammad Talha, SofianeKharbech and Wei Xiang, “Novel Medical Image Encryption Scheme Based on Chaos and DNA Encoding”, DOI 10.1109/ACCESS.2019.2906292, IEEE Access.

[5] Saleh Ibrahim, HeshamAlhumyani, MehediMasud, Sultan S Alshamrani, and M. Shamim Hossain, “Framework for Efficient Medical Image Encryption using Dynamic S-Boxes and Chaotic Maps”, VOLUME XX, 2020, PP 1-9, Digital Object Identifier 10.1109/ACCESS, 2020.

[6] Tahir Sajjadsli and Sashid Ali, “A Novel Medical Image Signcryption Scheme Using TLTS and Henon Chaotic Map”, VOLUME 8, PP 71974-71992, Digital Object Identifier 10.1109/ACCESS.2020.2987615, 2020.

[7] BehrouzVaseghi, Saleh Mobayen, SeyedehSomayehHashemi, and AfefFekih, “Fast Reaching Finite Time synchronization Approach for Chaotic Systems with Application in Medical Image Encryption”, VOLUME 9, 2021, PP 25911-25925, Digital Object Identifier 10.1109/ACCESS.2021.3056037,

[8] Mohammad KamrulHasan, Shayla Islam, RossilawatiSulaiman, and MdArif Hassan, “Lightweight Encryption Technique to Enhance Medical Image Security on Internet of Medical Things Applications”, VOLUME 9, 2021, PP 47731-47742, Digital Object Identifier 10.1109/ACCESS.2021.3061710,

[9] Yi Ding, Fuyuan Tan, Zhen Qin, and Mingsheng Cao, “DeepKeyGen: A Deep Learning-Based Stream Cipher Generator for Medical Image Encryption and Decryption”, 2162-237X © 2021 IEEE.

[10] Un Sook Choi, Sung Jin Cho and Sung Won Kang, “Color Medical Image Encryption Using 3D Chaotic Cat Map and NCA”, 978-1-7281-1542-9/19/$31.00 ©2019 IEEE.

[11] Baoru Han, YuanyuanJia, Guo Huang, and LishaCai, “A Medical Image Encryption Algorithm Based on Hermite Chaotic Neural Network”, PP 2644-2648, 978-1-7281-4390-3/20/$31.00 ©2020 IEEE.

[12] Sahar Haddad, GouenouCoatrieux, Alexandre Moreau-Gaudry, and Michel Cozic, “Joint Watermarking-Encryption-JPEG-LS for Medical Image Reliability Control in Encrypted and Compressed Domains”, PP 2556-2569, 1556-6013 © 2020 IEEE.

[13] Sara T. Kamal, Khalid M. Hosny, and Mostafa M. Fouda, “A New Image Encryption Algorithm for Grey and Color Medical Images”, VOLUME 9, 2021, PP 37855-37865, Digital Object Identifier 10.1109/ACCESS.2021.3063237.

[14] Jalaluddin Khan, Jianping Li, Amin UlHaq, ShadmaParveen and Sana Ullah, “medical image encryption into smart healthcare IoT system”, PP 378- 382, 978-1-7281-4242-5/19/$31.00©2019 IEEE.

[15] Yi Ding, Guozheng Wu, Dajiang Chen, and Ning Zhang, “DeepEDN: A Deep Learning-based Image Encryption and Decryption Network for Internet of Medical Things”, DOI 10.1109/JIOT.2020.3012452, IEEE.

[16] Prema T. Akkasaligara and SumangalaBiradar, “Selective medical image encryption using DNA cryptography”, VOL. 29, NO. 2, 91–101, DOI: 10.1080/19393555.2020.1718248.

[17] RichaMaurya, Ashwani Kumar Kannojiya, and Rajitha B, “An Extended Visual Cryptography Technique for Medical Image Security”, PP 415-421, ISBN: 978-1-7281-4167-1, 2020

[18] Sumit Kumar, BhaskarPanna, and Rajib Kumar Jha, “Medical image encryption using fractional discrete cosine transform with chaotic function”, https://doi.org/10.1007/s11517-019-02037-3, 11 September 2019, Springer

[19] S. Priya, and B. Santhi, “A Novel Visual Medical Image Encryption for Secure Transmission of Authenticated Watermarked Medical Images”, https://doi.org/10.1007/s11036-019-01213-x, 09 February 2019, Springer

[20] Zeesha Mishra and Bibhudendra Acharya, “High throughput and low area architectures of secure IoT algorithm for medical image encryption”, https://doi.org/10.1016/j.jisa.2020.102533, 2020, Elsevier.

[21] AashiqBanu S, and RengarajanAmirtharajan, “A robust medical image encryption in dual domain: chaos-DNA-IWT combined approach”, https://doi.org/10.1007/s11517-020-02178-w, 21 April 2020, Springer

[22] Xiuli Chai, Jitong Zhang, ZhihuaGan, and Yushu Zhang, “Medical image encryption algorithm based on Latin square and memristive chaotic system”, https://doi.org/10.1007/s11042-019-08168-x, 17 October 2019, Springer.

[23] Joshua C. Dagadu, Jian-Ping Li, and Emelia O. Aboagye, “Medical Image Encryption Based on Hybrid Chaotic DNA Diffusion”, https://doi.org/10.1007/s11277-019-06420-z, 25April 2019, Springer.

[24] Ghazanfar Farooq Siddiqui, Muhammad Zafar Iqbal, Khalid Saleem, Zafar Saeed, Adeel Ahmed Ibrahim, Hameed And Muhammad Fahad Khan, “A Dynamic Three-Bit Image Steganography Algorithm for Medical and e-Healthcare Systems”, Vol. 8, IEEE Access, Sept 2020.

[25] Lopez,Martinez,Hernandez, Palacious, V. Madina, “A stegnography Method using Neural Networks”, IEEE, Latin America transactions,Vol 18, March 2020.

[26] J. Tao, S. Li, X. Zhang, and Z. Wang, ‘‘Towards robust image steganography,’’ IEEE Trans. Circuits Syst. Video Technol., vol. 29, no. 2, pp. 594–600, Feb. 2019.

[27] S. Li and X. Zhang, ‘‘Toward construction-based data hiding: From secrets to fingerprint images,’’ IEEE Trans. Image Process., vol. 28, no. 3, pp. 1482–1497, Mar. 2019.

[28] M. Elhoseny, G. Ramírez-González, O. M. Abu-Elnasr, S. A. Shawkat, N. Arunkumar, and A. Farouk, ‘‘Secure medical data transmission model for IoT-based healthcare systems,’’ IEEE Access, vol. 6, pp. 20596–20608, 2018.