Journal of Artificial Intelligence in Medical Applications (JAIMA)
Vol. 1, No. 1, 2025, **pp**. 126–134
ISSN: 3106-1494 | **DOI**: https://doi.org/10.65511/jaima.v1i1.743

Secure Brain MRI Encryption Using RNA Encoding and Substitution-Permutation Network

Omar Fitian Rashid[1,*], Mohammed Ahmed Subhi[2], Sawal Md. Ali[3]

[1]Department of Geology, College of Science, University of Baghdad, Baghdad, 10011, Iraq; omar.f@sc.uobaghdad.edu.iq
[2] Department of Planning, Directorate of Private University Education,
Ministry of Higher Education and Scientific Research, Baghdad, 10011, Iraq; mohd.subhi@ik.edu.iq
[3]Faculty of Engineering and Built Environment, Universiti Kebangsaan Malaysia, Selangor, 43600, Malaysia; sawal@ukm.edu.my

Received: 16/09/2025, Revised: 05/11/2025, Accepted: 26/11/2025, Published: 30/12/2025

ABSTRACT: The increasing use of digital brain imaging in clinical diagnosis and telemedicine has raised serious concerns regarding the security and privacy of sensitive patient data. Traditional cryptographic methods may fail to provide adequate protection when handling large image sets or when additional semantic obfuscation is required. In this paper, we present a lightweight cryptographic framework for securing medical brain MRI images, based on a hybrid bio-inspired and cryptographic methodology. The architecture combines an RNA-based encoding scheme and a Substitution Permutation Network (SPN), which with high probability ensures high confusion and diffusion in the ciphertext and is compatible with biomedical data formats. Brain MRI images are mapped to a symbolically encoded RNA representation, placing each 8-bit grayscale pixel into a six-character RNA block, via custom encoding tables. The result of this representation is encrypted by a multi-round SPN cipher using a biologically inspired S-box, and a RNA-specific permutation plan. The decryption process merely inverts the SPN operations and the original image reinvents itself with no loss. Experimentally, the proposed method was tested on a Kaggle data set of brain tumor MRI images with glioma, meningioma, pituitary, and no-tumor cases. Findings indicate that 256×256 image encryption and decryption can be achieved in less than one second, which makes the framework appropriate to the telemedicine application of encryption and decryption in real time. In general, the encryption process proposed can be considered an effective and very secure system of protection of sensitive medical images.

Keywords: Medical image encryption, Brain MRI security, RNA encoding, Substitution-Permutation Network, Biological cryptosystem.

1. INTRODUCTION

The intensive development of telemedicine, cloud-based diagnostic, and digital health records has made medical imaging data, especially brain magnetic resonance imaging (MRI) datasets, one of the major objects of cyber-attacks and privacy breaches. MRI images of brain are very sensitive data which is very significant in diagnosis of neurological disorders such as tumours, cerebrovascular disease and neurodegenerative disorders [1][2]. Although the new technological progress has made healthcare services more affordable and accessible, it has also resulted in the sharpness of the urgent problems of privacy, data integrity, and safe working with patient-sensitive information [3]. The same level of confidentiality requirements depends on the ethical considerations as it does on the legal considerations in the Health Insurance Portability and Accountability Act (HIPAA) of the United States and the General Data Protection Regulation (GDPR) of the European Union [4] concerning medical images. The unlawful transfer of medical imaging data can cause loss of identity, prejudice, and abuse of personal data, hence, undermining the well-being of the patient. Given that the acquisition in brain MRI may produce complex anatomical information, the tradeoff or loss of this information may have colossal impacts on individuals and medical organizations. Telemedicine, in turn, is increasingly relying on real-time image transmission, which implies that the usage of strong and high-performance encryption systems is the inevitable consequence [5][6].

The fast evolving digital imaging technologies have fundamentally changed the clinical diagnosis and Telemedicine particularly in the area of brain MRI analysis. The result of these imaging modalities are voluminous amounts of high sensitivity information that are routinely uploaded and stored in networks to be accessed in medical consultation, diagnostic review, and research. In as much as such practices are necessary in enhancing access and efficiency within the healthcare continuum, they present high risks in the context of data security and patient confidentiality. Breaking into, robbing, or influencing the medical images could be the catalyst of disastrous adverse events, including wrong diagnosis, breach of patient privacy, and potential abuse of the clinical information. Although traditional cryptographic algorithms can be effective in most settings, they may not be suitable to address the special needs of medical imaging because image datasets are highly dimensional, real-time processing may be of paramount importance, and semantic faithful

requirements are mandatory [2]. Widely used cryptographic primitives, such as Advanced Encryption Standard (AES), Data Encryption Standard (DES), and RSA are successfully used to encrypt text and numeric information, but they are challenged with major challenges when applied to encrypt medical images. Brain MRI images are typically large and to maintain diagnostic value, fast lossless processing is required. The classical algorithms can be a significant increase of the computational tax, and thus unacceptable latency in real time telemedicine. In addition, these methods also fail to accommodate the structural and semantic subtleties, which clinicians count on, thereby compromising the quality of the information. This is further compounded by the huge storage and transmission implications of the high-resolution medical images which impose additional limitations on the traditional cryptographic methods. Collectively these constraints underscore the reality that generic encryption strategies cannot be applied to deliver sufficient security to sensitive medical images and the necessity to develop special domain specific security constructions that integrate bio-inspired techniques with modest cryptography paradigms. These plans are aimed at offering effective security, and simultaneously improving efficiency and reasonable compatibility with the current biomedical data formats. One of the possible approaches is the symbolic RNA-based encoding schemes that are built on cryptographic primitives, where the complexity of biological systems is used to enhance the security of data. These techniques may contain potent confusion and diffusion properties, founded on the application of Substitution Permutation Networks (SPNs), thereby discouraging the common cryptanalytic assaults. In this paper, we propose a novel hybrid bio-inspired and cryptographic architecture particularly in the protection of brains MRI images. The design is so that it makes real-time execution in secure telemedicine environments as well as preserve data fidelity and diagnostic quality The implementation of symbolic RNA-based encoding schemes and cryptographic primitives is one such promising direction where the intricacy of biological system is exploited to enhance the security of data. These combined with Substitution Permutation Networks (SPNs) can have strong confusion and diffusion, and they should be resistant to common cryptanalytic attacks. In the current paper, a hybrid bio-inspired cryptography system is proposed to offer brain MRI image security to achieve real-time operative in the framework of secure telemedicine, yet the integrity of data and diagnostic information is not compromised. The main contributions of the proposed method are summarized as follows:

1. An innovative RNA-based symbolic encoding system is developed to encode grayscale MRI images into nucleotide-like sequences to allow biologically inspired cryptography.
2. A lightweight Substitution-Permutation Network (SPN) is combined with RNA encoding to provide high confusion and diffusion at low computational cost.
3. The encryption mechanism proposed has a lossless decryption mechanism, which guarantees medical image integrity to be used in diagnoses.
4. The method is real-time (less than 1 second at 256 x 256 MRI images), which qualifies it as safe over the telemedicine environment.
5. The Kaggle Brain Tumor MRI dataset of glioma, meningioma, pituitary and no-tumor images is widely validated.
6. A high-quality semantic obfuscation is presented, which is resistant to statistical and brute-force cryptanalysis.

The rest of this manuscript is organized as follows: Section 2 reviews the related works on medical image encryption and bio-inspired cryptographic techniques. Section 3 presents the proposed methodology, including RNA-based encoding and SPN encryption. Section 4 provides the experimental results and discussion. Finally, Section 5 concludes the paper with remarks and outlines possible future work directions.

2. RELATED WORKS

The protection of medical images has been undertaken using conventional cryptographic algorithms such as the Advanced Encryption Standard (AES) and Rivest Shamir Adleman (RSA) with some degree of effectiveness [7][8]. Although such schemes are mathematically sound, they are often not designed to deal with the large size and huge redundancy of medical images. Any large volume of high-resolution MRI scans encrypted using these conventional methods may require significant computational cost, extend run time and may not even be compatible with standard medical data formats [9]. In addition, the generic cryptographic methods provide weak semantic obfuscation: even partially encrypted images can reveal distinguishable anatomical features to an enemy [7]. To overcome these limitations, researchers have progressively sought domain specific, bio-inspired encryption approaches which are customized to the unique characteristics of biomedical data [10]. Chaotic maps [11], DNA- and RNA-based coding schemes [12][13], and lightweight substitution permutation networks [14] have all proven to be useful both in enhancing security and computational efficiency. In particular, bio-inspired mechanisms, will use symbolic representations of

biological systems to provide yet another level of complexity to increase vulnerability to statistical and brute-force attacks [15].

On the basis of these advances, the current paper presents a new hybrid cryptographic architecture that is used to secure brain MRI images. The suggested algorithm combines symbolic RNA-based coding with a multi-round substitution-permutation network (SPN), comprising of biologically inspired substitution rules, and tailored permutation patterns. Here every pixel of the grayscale MRI image is encoded into a symbolic RNA sequence, then it repeatedly substituted and permutated to accomplish strong confusion and diffusion qualities in the encrypted text. Unlike other schemes, the suggested system ensures that the original image is reconstructed without any loss, but allows encryption and decryption of the image in real time, which makes it especially advantageous in telemedicine implementations. The effectiveness of the approach in cryptographic strength and computational efficiency is evidenced by experimental studies that were performed on the Kaggle brain tumor MRI dataset. The summary of the related works is presented in Table 1.

Table 1. Summary of Related Works on Medical Image Encryption

Author Reference	Method	Dataset	Main Technique	Advantages	Limitations
Basha et al. [6]	IoT-healthcare encryption	Brain tumor images	Puzzle sine cosine optimization	Optimized security	Higher time complexity
Lata et al. [7]	Classical cryptography (AES)	General medical images	Strong mathematical foundation	Widely tested	High computational cost, limited semantic security
Singh et al. [8]	Classical cryptography (RSA)	General medical images	Strong mathematical foundation	Widely tested	High computational cost, limited semantic security
Belazi et al. [11]	Chaotic map	Telemedicine images	Sine-derived chaotic maps	Lightweight, secure	Sensitive to parameter tuning
Proposed method	RNA + SPN	Brain MRI (Kaggle)	Hybrid bio-inspired + SPN	Real-time, lossless decryption, strong semantic security	Limited to grayscale MRI, fixed image size

Current approaches to encryption of medical images have been associated with a high level of strengths, and at the same time, have been faced with significant weaknesses. Modelling techniques such as sine-cosine models are often very practical in terms of security but require high time complexity, making them unrealistic at real-time operation. Classical cryptographic designs, such as AES and RSA, which are mathematically correct and have been well-tested, are computationally-intensive and do not provide sufficient protection to the semantic integrity of medical images. The approaches based on chaotic maps provide relatively low-weight security; they however, are very sensitive to parameter tuning, which limits their reliability in dynamic healthcare. In order to alleviate these shortcomings, the suggested RNA+SPN framework presents a bio-inspired coding scheme, alongside substitution-permutation operations that allow to achieve rapid, lossless encryption and strong confusion, diffusion, and semantic protection. Unlike conventional methods, the method is specific to grayscale MRI data and can facilitate real-time secure transmission, making it a viable and reliable tool in the case of telemedicine use.

3. METHODOLOGY

This study presents a new multi-layered encryption approach to brain MRI images based on genetic coding and a Substitution Permutation Network. The process begins with a confusion layer, where image bytes are encoded into RNA sequences before applying the Substitution Permutation Network. This design adds security and creates more complexity, thus making the unauthorized decoding significantly harder. The method has been tested using standard brain MRI data, using histogram analysis, entropy measure, and pixel correlation tests. The main reason to protect medical images is to uphold patient privacy and confidentiality and maintain clinical integrity. Deliberate malformations of medical scans, including the changes in the area of tumors or the details of the diagnosis, can lead to the wrong clinical decision, and patient life can be in danger. Besides, as remote diagnosis and mobile consultation services become more common, medical pictures are often transferred over open networks, in which encryption is invaluable in the process of securing its safety. Proposed encryption framework is depicted in Figure 1.

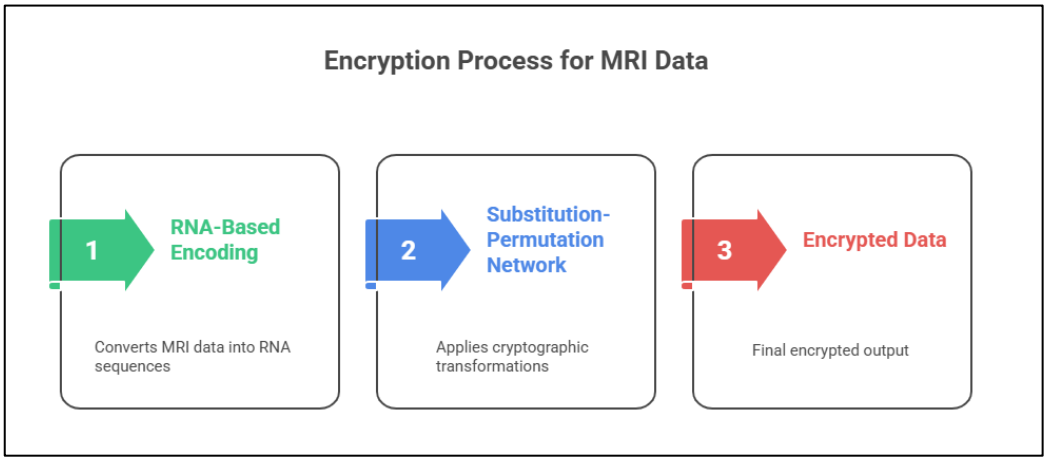

Figure 1. The proposed encryption steps

3.1. Dataset

The dataset used is the Kaggle Brain Tumor MRI Dataset, where this dataset has various grayscale images for MRI scans of the brain. This Kaggle data is a complete brain tumor classification training and testing resource. Different images that include various brain section are used as input for the proposed method. Where each image has made of pixels, each pixel has a value between 0 and 255. Where the key specifications of the Kaggle Brain Tumor MRI Dataset are presented in Table 2.

Table 2. Key specifications of the Kaggle Brain Tumor MRI Dataset

Feature	Details
Classes	Glioma, Meningioma, Pituitary Tumor, No Tumor
Number of Images	7,023
Primary Sources	Kaggle (composite of multiple datasets)
Preprocessing	Resize images, remove duplicates, address mislabels
Image Size (preprocessed)	Often standardized to 224 × 224 pixels for deep learning tasks
Typical Split	Commonly structured as 80% training / 20% evaluation Approximation 5,600 training and 1,400 testing images

3.2. RNA-Based Encoding

In this phase, a layer of biological transformation is introduced prior to encryption. Encoded in form of RNA, inspired by the process of encoding genetic information in the form of a two-letter codon composed of nucleotides in a set of (A, U, C, G), each byte (0 255) is assigned a six-letter codon. Where the process of encoding for every byte (8 bits) are as follows:

- Transform Brain Tumor image to grayscale image with 8-bit binary string.
- Divide this string into:
  - First 2 bits → maps these two bits to the first two nucleotides, and the encoding is done based on Table 3.
  - Next 3 bits → maps these three bits to the second two nucleotides, and the next encoding is done using the encoding shown in Table 4.
  - Last 3 bits → maps the last three bits to third two nucleotides, also done using RNA encoding mentioned in the Table 4.

Table 3. RNA encoding for the first 2 bits

Bit Sequence	Nucleotide
00	AA
01	UU
10	CC
11	GG

Table 4. RNA encoding for the 3 bits

Bits	Nucleotide
000	AC
001	UA
010	CA

011	GA
100	AG
101	UC
110	CU
111	GU

In this phase, each byte is encoded uniquely as a codon such as AAACAC, where the end product is less stream of codons compared to the initial byte stream. Table 5 show an example of RNA encoding for the byte's values.

Table 5. RNA encoding for the entire byte

Decimal	Binary	RNA Encoding
0	00000000	AAACAC
1	00000001	AAACUA
2	00000010	AAACCA
3	00000011	AAACGA
4	00000100	AAACAG
5	00000101	AAACUC
6	00000110	AAACCU
7	00000111	AAACGU
8	00001000	AAUAAC
9	00001001	AAUAUA
10	00001010	AAUACA
…	…	…
255	11111111	GGGUGU

3.3. Substitution-Permutation Network

Substitution-Permutation Network (SPN) is a traditional symmetric encryption network that is implemented in a lot of modern block ciphers. It puts on alternate layers of:

- Substitution (confusion): it substitutes a set of symbols with another set with the help of a look-up table (S-box)
- Permutation (diffusion): rearranges the symbols to disseminate the impact of modifications

This structure produces a formidable equilibrium between security and performance and it is generally applicable to lightweight or symbol-based encryption systems. In the proposed method, each byte of the image is encoded to 6-character RNA sequence based on building RNA encoding tables. The RNA blocks are then subjected to a number of SPN rounds as shown below:

- Step 1 Substitution: in this step, the RNA characters is divided to codons (triplets), e.g., AAC, GCU, etc. Where each codon is replaced by an RNA-based S-box, which maps codons to new codons, e.g., AAC to UGU, GCU to CGA, etc.
- Step 2 Permutation: in this step, RNA characters are substituted (not the codons, but the single letters) are then re-arranged according to predetermined permutation rule, and this is done to guarantee diffusion, whereby a little modification in the input influences a lot of output symbols.
- Step 3 Repeat for multiple rounds: in this step, repeat the substitution and permutation three times (rounds).

The proposed encryption method is illustrated in Algorithm 1.

Algorithm 1: The proposed encryption method

Input:
Grayscale medical image (I) of size (M×N), where each pixel ∈ [0, 255]
RNA encoding tables (Table 1 and Table 2)
Codon S-Box (Sbox)
Permutation Vector (P)
Number of SPN Rounds (r)

Output: Encrypted RNA sequence (I_enc)

Step 1: for each pixel p in the image I:
1.1 Convert p to 8-bit binary format
1.2 Split into three segments:

- First 2 bits → Encode using RNA Table 1 → 2 RNA characters
- Next 3 bits → Encode using RNA Table 2 → 2 RNA characters
- Last 3 bits → Encode using RNA Table 2 → 2 RNA characters

1.3 Combine the three RNA parts → RNA_block (length = 6 characters)

Step 2: apply SPN encryption for each RNA_block:

For round = 1 to r:
2.1 Substitution:
Split RNA_block into two codons (3 characters each)
Replace each codon using Sbox
2.2 Permutation:
Rearrange the 6 RNA characters using permutation vector P
2.3 Update RNA_block with substituted and permuted result

Step 3: added each encrypted RNA_block to I_enc

Step 4: return I_enc as the final encrypted RNA sequence

3.4. Parameters of the Proposed Method

The main parameters used in the proposed method are as follows:

- Image size: 256×256 grayscale MRI images.
- Encoding tables: RNA mapping (Table 2 & 3).
- Codon S-box: Biologically inspired substitution table.
- Permutation vector (P): e.g., [2, 0, 5, 4, 3, 1].
- Number of SPN rounds (r): 3 rounds.
- Dataset: Kaggle Brain Tumor MRI Dataset (glioma, meningioma, pituitary, no-tumor).
- Execution environment: Standard PC, single CPU processing.

3.5. Decryption Process

The reverse process of the encryption process is the exact decryption stage of the proposed RNA-based Substitution-Permutation Network (SPN) cipher. The decryption process starts with the coded RNA sequence, usually in codon triples, and processes the changes, made at encryption in reverse order. The process guarantees the correct reconstruction of the original pixel values that were originally encoded on the RNA allowing complete recovery of the image. Firstly, a reverse of permutation is done, where the permutation is a fixed rearrangement of characters according to a known pattern the same permutation vector used in the encryption process is used in reverse. As an example, the permutation of encryption could be [2, 0, 5, 4, 3, 1], and the inverse permutation restores the characters in their initial location. This is to replace the codons back into their original ordering in each block before the permutation.

After the inverse permutation, the cipher does the inverse substitution based on the reverse S-box. The permuted RNA sequence is compared to the output values of the S-box in order to determine which input codon corresponds to each codon. This reverses the original codons pre-substitution. The correctness of this step can be verified by a bijective (one-to-one) mapping of the S-box construction to ensure that each of the encrypted codons will have a unique original codon counterpart. The process of substitution and reversal of permutation is then repeated in the same order backward in all rounds of encryption. As an example, consider that three rounds of SPN were used when encrypting, so when decrypting, the inverse permutation and inverse S-box of round 3 are applied first, then round 2 and then round 1. Such strict order is obligatory since the SPN structure implies using transformations of compounds as at each step the result of the previous one is used to form the current one. When all the SPN rounds have been reversed, the RNA blocks are decrypted and recombined to form a complete RNA encoded sequence. Lastly, the RNA-to-byte decoding is used. The

second step is the parsing of each of the 6-character blocks of RNA into three parts, the first two characters of which are used to determine the first 2 bits using Table 1, and the next 2 characters blocks are used to decode the rest of the 6 bits using Table 2 to decode the 3 bits. The RNA blocks are in turn decoded back to their initial 8-bit binary representation and finally, to pixel value.

The entire decryption process makes it fully reversible, lossless recovery of images, and high integrity of data. It can also be used to store and transfer confidential medical images, including a brain MRI, and be encrypted symbolically (through RNA).

4. RESULTS AND DISCUSSION

The Kaggle Brain Tumor MRI dataset has four image groups, which are glioma tumor, meningioma tumor, no tumor, and pituitary tumor, an example for these images are shown in Figure 2.

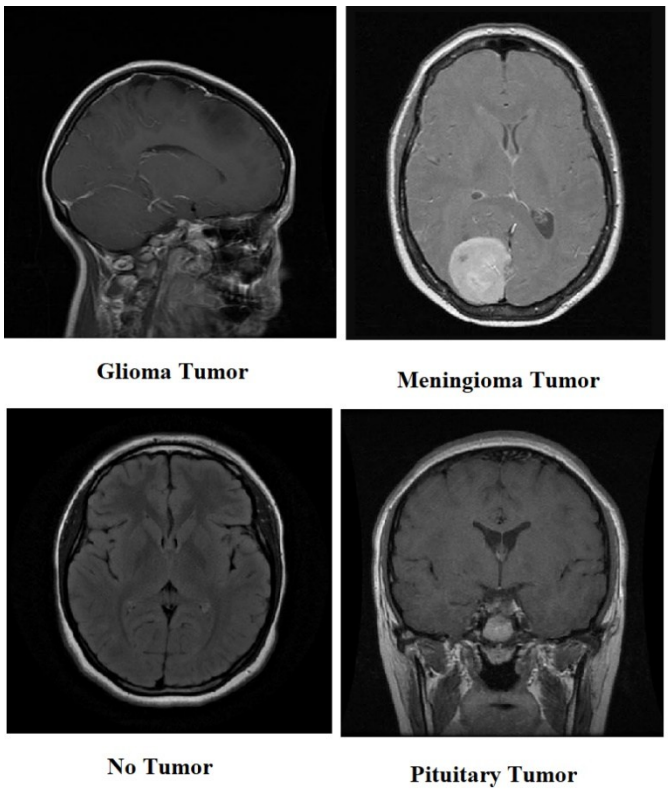

Figure 2. The Kaggle Brain Tumor MRI dataset images types

The performance evaluation of the proposed system is done by calculating execution time for all training dataset image types, the execution time includes: encoding time (the time needed to convert image pixel to RNA sequence), encryption time (time needed to applied Substitution-Permutation Network), decryption time (the required time to inverse SPN), and decoding time (time to convert RNA sequences to byte). The execution time of the proposed method is listed in Table 6 and Figure 3.

Table 6. Execution time for Brain Tumor MRI dataset images (256×256)

Image Type	Encoding time (s)	Encryption time (s)	Decryption time (s)	Decoding time (s)	Total time (s)
Glioma Tumor	0.148	0.298	0.305	0.142	0.893
Meningioma Tumor	0.139	0.291	0.309	0.134	0.873
No Tumor	0.137	0.286	0.301	0.130	0.854
Pituitary Tumor	0.141	0.294	0.307	0.136	0.878

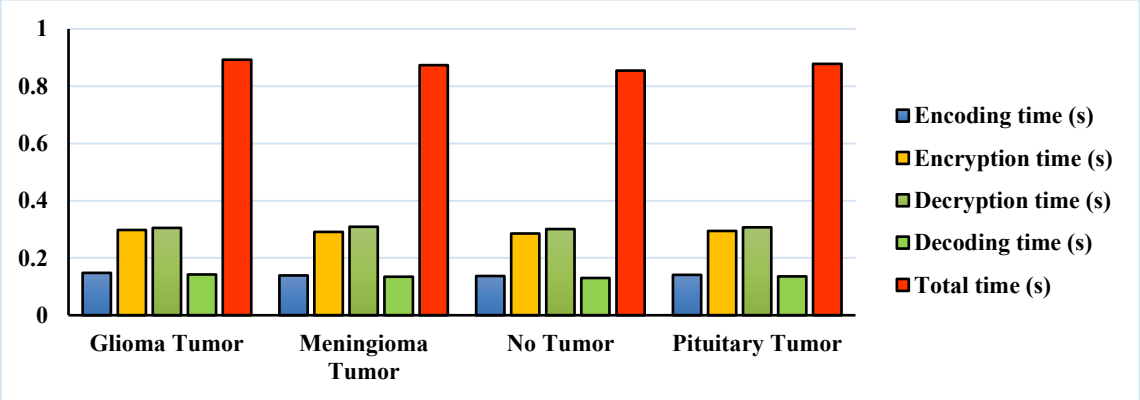

Figure 3. Execution time for Brain Tumor MRI dataset images (256×256)

In order to understand the encryption process, the following example illustrate the encoding and SPN encryption on a single image pixel value, and these steps are repeated for all image pixels:

- Image pixel value: is equal to 197
- Binary (8-bit): 11000101

Step 1: RNA Encoding:
Split into 3 parts:

- First 2 bits: 11 → Table 3 → GG
- Next 3 bits: 000 → Table 4 → AC
- Last 3 bits: 101 → Table 4 → UC

So, the RNA encoding: GGACUC
Step 2: SPN Encryption:
Define a mock S-box as shown in Table 7.

Table 7. An example of S-box

Input	Output
GGA	UCU
CUC	AGG
ACA	UGC
GAC	CGA
ACU	AAG
…	…

- Split codon into triplets: GGA | CUC
- Substitution via S-box: GGA → UCU, CUC → AGG
- Resulting: UCUAGG

Applied permutation rule, for example: [5, 2, 0, 4, 1, 3]
Apply to "UCUAGG":

- Original: U C U A G G
- Reordered: G U U G C A

Repeat the same process (new S-boxes and permutations) for round two and three.
Output: encrypted RNA sequence

4.1. Limitations of the Study

Even though the suggested encryption approach is showing promising results, it is not entirely limited:

- The test was restricted to grayscale brain MRI images; an extension of the test to color medical images is one of the possible directions to explore in the future.
- The approach was only tested on fixed-sized images (256 256); further optimization will be required to scale up to larger sizes of the images.

- Experimental validation was only on the Kaggle dataset; a thorough evaluation using real-world clinical datasets that are more heterogeneous should be considered.

5. CONCLUSION

A new bio-inspired encryption method is introduced to protect brain MRI images with the combination of the RNA-based symbolic encoding technique and a Substitution-Permutation Network. The system differs with traditional numerical cryptographic systems by working directly on nucleotide-like sequences of characters unlike the common cryptographic systems which works on the numeric set of characters. The grayscale images mapped into RNA sequences through a custom mapping scheme in which the 8-bit pixel segments were mapped into biologically realistic RNA characters. These symbolic RNA blocks were then used in an SPN (Substitution-Permutation Network) architecture, with S -blocks derived biologically and fixed permutation rules used. The resultant structures therefore had high confusion and diffusion properties. The suggested algorithm was tested on the Kaggle Brain Tumor MRI Dataset which includes a broad range of the tumour types, such as glioma, meningioma, pituitary, and cases that do not have the tumours. The overall execution time was less than one second on average on standard 256*256 medical images, and thus demonstrates the applicability of the method to real-time clinical implementation. RNA level encoding combined with SPN based cryptographic processing is not only the sole means of ensuring a high level of data confidentiality, but also a new semantic level of obfuscation that has the potential to give resistance to new cryptanalytic methods. Therefore, the potential of the proposed system as a secure transmission of medical images, cloud storage, and telemedicine uses can be very promising because of its effectiveness, efficiency, and biological interpretability. For future work, can broaden the research approach to colour medical images by implementing the RNA encoding and SPN transformation to each channel of the RGB colour space separately. This would expand the range of the approach to a broader range of diagnostic imaging modalities.

REFERENCES

[1] Y. Wang, H. Xiong, K. Sun, S. Bai, L. Dai, Z. Ding, J. Liu, Q. Wang, Q. Liu, and D. Shen, "Toward general text-guided multimodal brain MRI synthesis for diagnosis and medical image analysis," *Cell Reports Medicine*, vol. 6, issue 6, 2025, https://doi.org/10.1016/j.xcrm.2025.102182.

[2] Y. Sailaja, and P. Velmurugan, "A novel feature extraction and deep spiking MobileNet for brain stroke detection using MRI image," *Engineering Applications of Artificial Intelligence*, vol. 159, part A, 2025, https://doi.org/10.1016/j.engappai.2025.111565.

[3] A. Baten, R. K. Biswas, E. Kendal, and J. Bhowmik, "Continuum of maternal healthcare services utilization in low-and middle-income countries: A multi-level analysis," *Midwifery*, vol. 149, 2025, https://doi.org/10.1016/j.midw.2025.104549.

[4] R. V. Rose, A. Kumar, and J. S. Kass, "Protecting Privacy: Health Insurance Portability and Accountability Act of 1996, Twenty-First Century Cures Act, and Social Media," *Neurologic Clinics*, vol. 41, issue 3, pp. 513-522, 2023, https://doi.org/10.1016/j.ncl.2023.03.007.

[5] A. D. Piersson, G. Nunoo, K. Dzefi-Tettey, and N. Otumi, "Utility of advanced brain MRI techniques for clinical and research purposes in a low-resource setting: A multicentre survey," *Next Research*, vol. 2, issue 3, 2025, https://doi.org/10.1016/j.nexres.2025.100638.

[6] S. M. Basha, J. Sreemathy, A. Arun, and S. Sureshu, "Puzzle sine cosine optimization-based secure communication and brain tumor classification in IoT-healthcare system," *Biomedical Signal Processing and Control*, vol. 102, 2025, https://doi.org/10.1016/j.bspc.2024.107261.

[7] K. Lata, C. Gupta, and L. R. Cenkeramaddi, "A cryptographic framework for secure medical imaging in smart healthcare environments," *Results in Engineering*, vol. 27, 2025, https://doi.org/10.1016/j.rineng.2025.106780.

[8] D. Singh, and S. Kumar, "Image authentication and encryption algorithm based on RSA cryptosystem and chaotic maps," *Expert Systems with Applications*, vol. 274, 2025, https://doi.org/10.1016/j.eswa.2025.126883.

[9] R. Frysch, T. Pfeiffer, and G. Rose, "A novel approach to 2D/3D registration of X-ray images using Grangeat's relation," *Medical Image Analysis*, vol. 67, 2021, https://doi.org/10.1016/j.media.2020.101815.

[10] E. Ni, E. Knight, and M. Gerstein, "Scalable and efficient on-chain data management in blockchain for large biomedical data," *Journal of Biomedical Informatics*, vol. 165, 2025, https://doi.org/10.1016/j.jbi.2025.104818.

[11] A. Belazi, and A. B. Mabrouk, "A refined sine-derived chaotic map for securing medical image encryption in telemedicine," *Computers in Biology and Medicine*, vol. 196, part A, 2025, https://doi.org/10.1016/j.compbiomed.2025.110667.

[12] O. F. Rashid, Z. A. Othman, S. Zainudin, and N. A. Samsudin, "DNA Encoding and STR Extraction for Anomaly Intrusion Detection Systems," *IEEE Access*, vol. 9, no. 2411, pp. 31892-31907, 2021, DOI: 10.1109/ACCESS.2021.3055431

[13] M. A. Subhi, O. F. Rashid, S. A. Abdulsahib, M. K. Hussein, and S. M. Mohammed, "Anomaly Intrusion Detection Method based on RNA Encoding and ResNet50 Model," *Mesopotamian Journal of CyberSecurity*, vol. 4, no. 2, pp. 120-128, 2024, DOI: 10.58496/MJCS/2024/011

[14] V. K, A. Karthik, G. C. Kamaleshwar, A. S. Kumar, V. S. Krishna, V. S. Ram, P. Yogesh, S. M. Verappan, and A. Prathiba, "Tower field construction of power attack resistant 4×4 substitutions in lightweight SPN ciphers for implantable medical devices," *Alexandria Engineering Journal*, vol. 128, pp. 767-785, 2025, https://doi.org/10.1016/j.aej.2025.07.030.

[15] S. Huang, S. Liu, D. Wang, S. Wu, G. Wang, L. Wan, Q. An, L. Zhu, and C. Li, "Bio-inspired cutting tools: Beneficial mechanisms, fabrication technology and coupling design," *Sustainable Materials and Technologies*, vol. 43, 2025, https://doi.org/10.1016/j.susmat.2024.e01211.