Concealed Image Encryption for Medical Images

Devansh Vikram
21BCE1554

Yashvi Bhatt
21BCE5056

ABSTRACT

Recently, diagnosing diseases using medical images has become crucial. As these images are transmitted through the network, they need a high level of protection. If the data in these images are liable for unauthorized usage, this may lead to severe problems. There are different methods for securing images. One of the most efficient techniques for securing medical images is encryption.

The concealed encryption and decryption algorithm proposed for grey and color medical images addresses a critical need for enhanced security during transmission.

Through innovative techniques such as image splitting, zigzag pattern scrambling, and chaotic key generation, the algorithm ensures robust encryption.

Comprehensive security analyses and a comparative study with existing methods validate its effectiveness, making it a valuable advancement in medical image encryption and decryption.

INTRODUCTION

The increasing reliance on medical imaging for disease diagnosis necessitates heightened protection for transmitted images to prevent unauthorized access and ensure patient privacy. Encryption emerges as a crucial solution, and a concealed encryption and decryption algorithm is proposed for grey and color medical images, integrating innovative techniques like image splitting, zigzag pattern scrambling, and chaotic key generation to enhance security.

Objectives include developing this algorithm, implementing innovative techniques for robust encryption, and conducting a comprehensive security analysis along with a comparative study to validate its effectiveness against existing methods.This algorithm promises to provide a reliable solution for safeguarding sensitive patient information and maintaining the integrity of diagnostic procedures.

This paper aims to:

- Develop a concealed encryption and decryption algorithm for grey and color medical images.
- Implement innovative techniques, including image splitting, zigzag pattern scrambling, and chaotic key generation, to enhance the robustness of the encryption.

- Conduct a comprehensive security analysis and perform a comparative study with existing methods to validate the effectiveness of the proposed algorithm

LITERATURE SURVEY

The algorithm operates through a series of stages, including encryption and decryption, each meticulously outlined for clarity. In the encryption phase, the algorithm divides the plain image into blocks, applies confusion through pixel arrangement manipulation, generates keys using a chaotic logistic map, and conducts diffusion to alter pixel values. The decryption phase reverses these steps, ensuring the recovery of the original image.

A notable aspect of the algorithm is its emphasis on randomness and security. Through entropy analysis, the randomness of the encrypted images is evaluated, with results demonstrating high entropy values near 8, indicating robust randomness essential for secure encryption. Furthermore, the algorithm's resistance to differential attacks is assessed through metrics such as NPCR and UACI, showcasing its ability to withstand attempts to infer information from slight changes in the plain image.The algorithm's effectiveness in preserving image quality while ensuring security is highlighted through various analyses.Histogram analysis confirms the uniform distribution of pixel values in encrypted images, preventing attackers from discerning image content. Additionally, correlation coefficient measurements reveal a significant reduction in correlation between adjacent pixels in encrypted images compared to their plain counterparts, signifying the algorithm's success in obscuring image patterns. Moreover, the algorithm's performance is evaluated across different parameters, including keyspace, key sensitivity, and encryption efficiency. The keyspace's size and sensitivity to key alterations are crucial for ensuring the algorithm's resilience against brute-force attacks and unauthorized access attempts. Results indicate a sufficiently large keyspace and sensitivity to key changes, reinforcing the algorithm's security measures.The algorithm's versatility is also demonstrated through its application to both grey and color medical images, with evaluations conducted across various image formats and sizes.Through comprehensive testing and analysis, the algorithm consistently exhibits strong encryption capabilities, maintaining high levels of security and preserving image quality across different image types and sizes. Its robust security measures, efficient encryption processes, and compatibility with different image types make it a promising solution for safeguarding sensitive medical data while maintaining image integrity.

System Architecture:

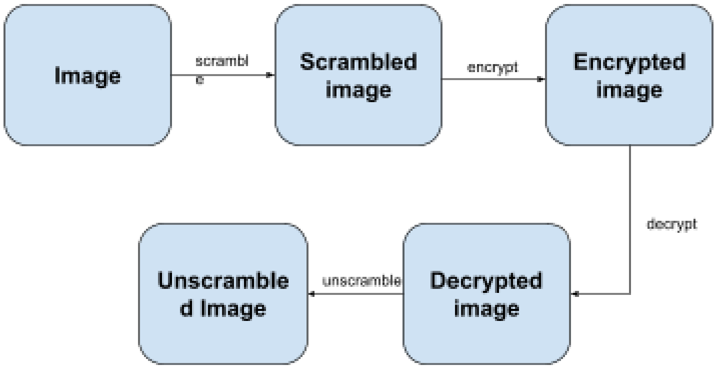


Figure 1.1

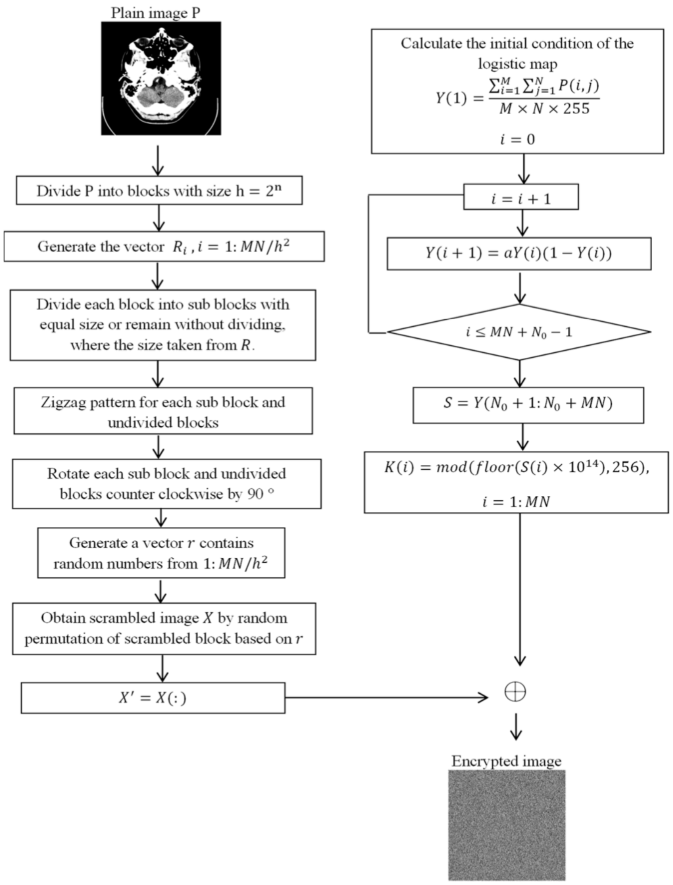

Plain image P
Divide P into blocks with size h = 2^n
Generate the vector R_i , $i = 1: MN/h^2$
Divide each block into sub blocks with equal size or remain without dividing, where the size taken from R.
Zigzag pattern for each sub block and undivided blocks
Rotate each sub block and undivided blocks counter clockwise by 90 °
Generate a vector r contains random numbers from $1: MN/h^2$
Obtain scrambled image X by random permutation of scrambled block based on r
$X' = X(:)$
Calculate the initial condition of the logistic map
$Y(1) = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N} P(i,j)}{M \times N \times 255}$
$i = 0$
$i = i + 1$
$Y(i+1) = aY(i)(1 - Y(i))$
$i \leq MN + N_0 - 1$
$S = Y(N_0 + 1: N_0 + MN)$
$K(i) = mod(floor(S(i) \times 10^{14}), 256)$,
$i = 1: MN$
$\oplus$
Encrypted image

Figure 1.2

Explanation:

Module 1-

In the first module, we perform image scrambling using confusion. Confusion is the process of changing pixels' arrangement in the image. In our algorithm, confusion is performed for blocks and sub-blocks as follows:

1. The zigzag pattern is applied to all the blocks, as described in Figure 2.

2. Both undivided blocks and sub-blocks rotated by 90°.

3. Random vector *r* generated where its size is equal to the number of blocks in the plain image.

4. Random permutation between blocks based on the vector *r* is applied to get the scrambled image.

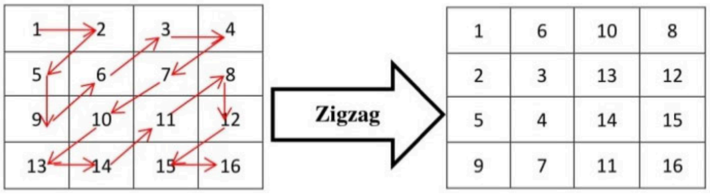


FIGURE 2. Demonstration of the zigzag pattern.

Figure 1.3

Module 2-

In the second module we perform image encryption. We first need a key for the same. The key used in the diffusion process is generated from the logistic map. The logistic map is defined by:

$$Y_{n+1} = aY_n (1 - Y_n)$$

Where r is the control parameter with the range $0 < a <= 4$, Yn is the output sequence with $0 < Y_n < 1$. The map is bifurcation diagram of the logistic map. The key generation steps are defined as follows:

1. Calculate the initial value of the logistic map that depends on the plain image P by the following equation:

$$Y_0 = \frac{\sum_{i=1}^{M} \sum_{j=1}^{N} P(i, j)}{M \times N \times 255}$$

The numbers, M and N, refer to the number of rows and columns in the plain image, respectively.

2. Iterate the chaotic map (eq.1) N0 + MN times, and then skip the first N0 elements to get a new sequence S with size MN.

3. Calculate the key using the following formula:

$$K(i) = \mathrm{mod}\left(\mathrm{floor}\left(S(i) \times 10^{14}\right), 256\right), \quad i = 1 : MN$$

chaotic when a ∈ [3.57,4]. Figure 3 shows the

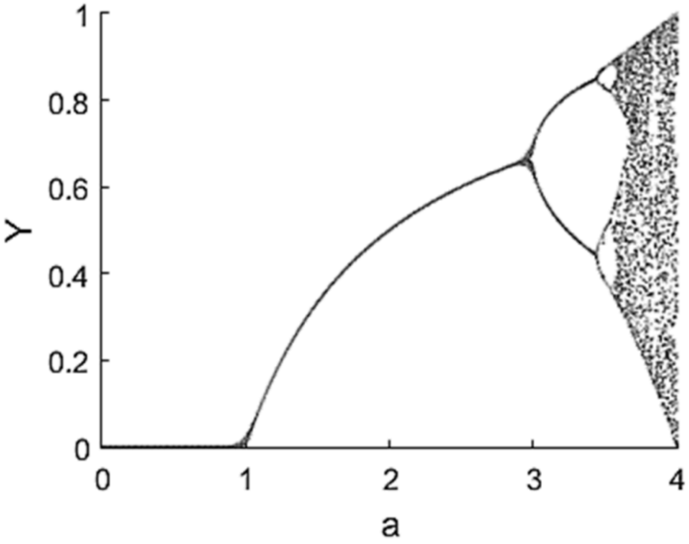


FIGURE 3. **Bifurcation diagram of the logistic map.**

Figure 2.1

In the diffusion process, image pixel values are changed, and then a noise image is generated. Bit-wise exclusive OR operation between the key *K* and the scrambled image vector is performed to obtain the encrypted image.

Module 3-

The third and the final module aims at the decryption and unscrambling of the image to get our original image back. With the original key and by inverting the encryption stages, we can retrieve the plain image. The decryption process is described as follows:

1. Bit-wise exclusive OR operation between the key *K* and the encrypted image vector is applied

3. The inverse operation of rotation and the zigzag pattern, respectively, are applied to both undivided blocks and sub-blocks.

Implementation:

Original Image:

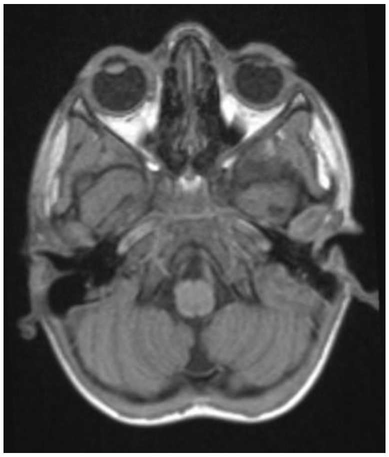
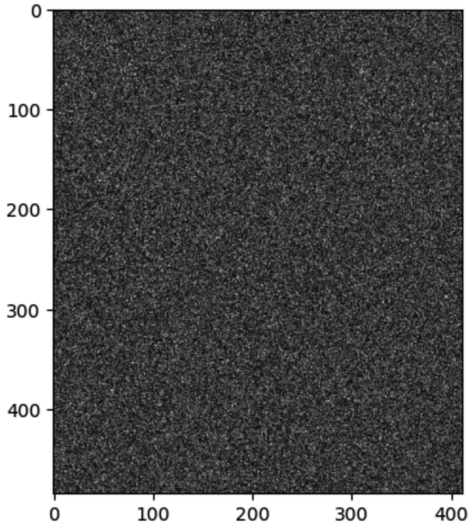


Figure 3.1

Scrambled Image:



to get the scrambled image.

2. Return each block to its original position using vector *r*.

Encrypted Image:

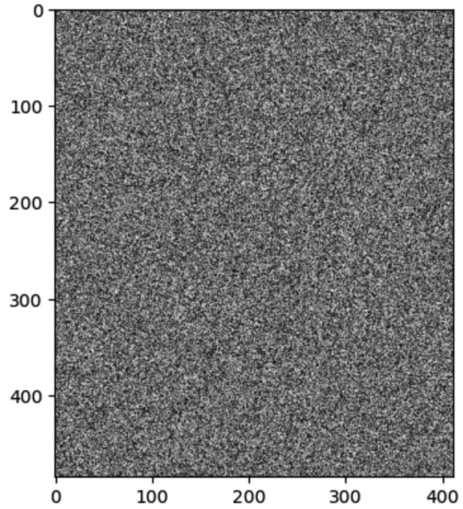


Figure 3.3

Decrypted Image:

Figure 3.2

Unscrambled Image:

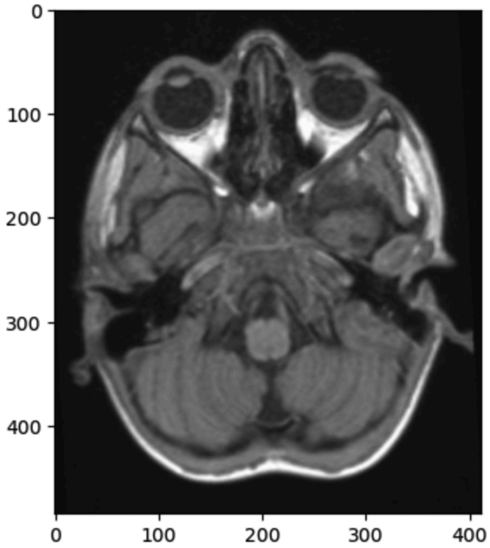


Figure 3.5

Conclusion:

In this paper, we present a novel algorithm to encrypt medical images via image blocks and chaos. The analysis performed illustrates the efficiency of the proposed algorithm in the encryption of grayscale and color medical images to guarantee their confidentiality and integrity.

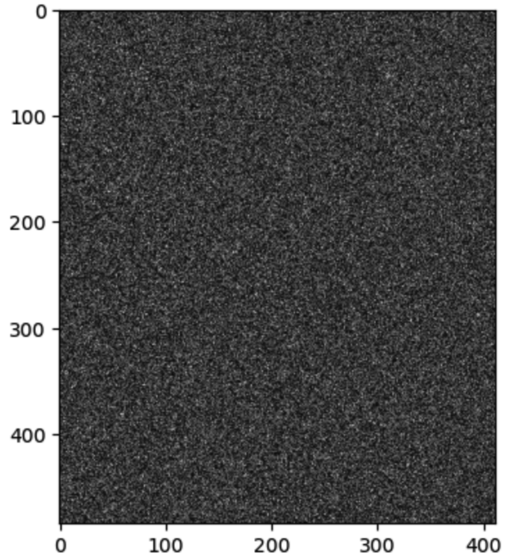


Figure 3.4

Future Work:

Future work related to the presented algorithm for encrypting medical images could focus on several avenues for further enhancement and exploration. Firstly, there could be efforts to optimize the algorithm's computational efficiency to ensure faster encryption and decryption processes, particularly when dealing with large volumes of medical image data. Additionally, research could delve into refining the algorithm's robustness against advanced cryptanalytic attacks, such as differential cryptanalysis or chosen-plaintext attacks, to bolster its security capabilities.

Furthermore, exploring the applicability of the algorithm to various modalities of medical imaging, such as MRI, CT scans, or ultrasound, could broaden its scope and utility within the medical imaging community. Integration with emerging technologies like blockchain for secure storage and transmission of encrypted medical images could also be a promising avenue for future investigation.Moreover, considering the increasing importance of privacy-preserving techniques in healthcare, further research could explore techniques for ensuring patient privacy while still enabling secure sharing and analysis of encrypted medical images, perhaps through techniques like homomorphic encryption or secure multi-party computation.

Additionally, conducting user studies or surveys to evaluate the usability and user experience of the algorithm in real-world clinical settings could provide valuable insights for refining the algorithm and making it more user-friendly for healthcare practitioners.

Overall, future work in this area could aim to advance the algorithm's performance, security, versatility, and usability, ultimately facilitating its adoption as a reliable tool for safeguarding sensitive medical image data in diverse healthcare contexts.

References:

[1] SARA T. KAMAL 1 , KHALID M. HOSNY 2 , (Senior Member, IEEE), TAHA M. ELGINDY 3 , MOHAMED M. DARWISH 1 , AND MOSTAFA M. FOUDA 4 , (Senior Member, IEEE) on A New Image Encryption Algorithm for Grey and Color Medical Images

[2] Vinod Kumar 1,2 & Vinay Pathak 3 & Neelendra Badal 4 & Purnendu Shekhar Pandey5 & Rajesh Mishra6 & Sachin Kumar Gupta7 on Complex entropy based encryption and decryption technique for securing medical images

[3] Ahmed A. Abd El-Latif; Bassem Abd-El-Atty; Muhammad Talha on Robust Encryption of Quantum Medical Images

[4] Walid El-Shafai, Iman Almomani, Anees Ara & Aala Alkhayer for An optical-based encryption and authentication algorithm for color and grayscale medical images.

[5] Ibrahim Yasser; Abeer T. Khalil; Mohamed A. Mohamed; Ahmed S. Samra; Fahmi Khalifa on A Robust Chaos-Based Technique for Medical Image Encryption

[6] Fawad Masood, Maha Driss, Wadii Boulila, Jawad Ahmad, Sadaqat Ur Rehman, Sana Ullah Jan, Abdullah Qayyum & William J. Buchanan on A Lightweight Chaos-Based Medical Image Encryption Scheme Using Random Shuffling and XOR Operations

CODE LINK-
https://drive.google.com/file/d/1xptAu8MBZ-GdkvNf6kdlXTCo5FXHdqMq/view?usp=drive_link