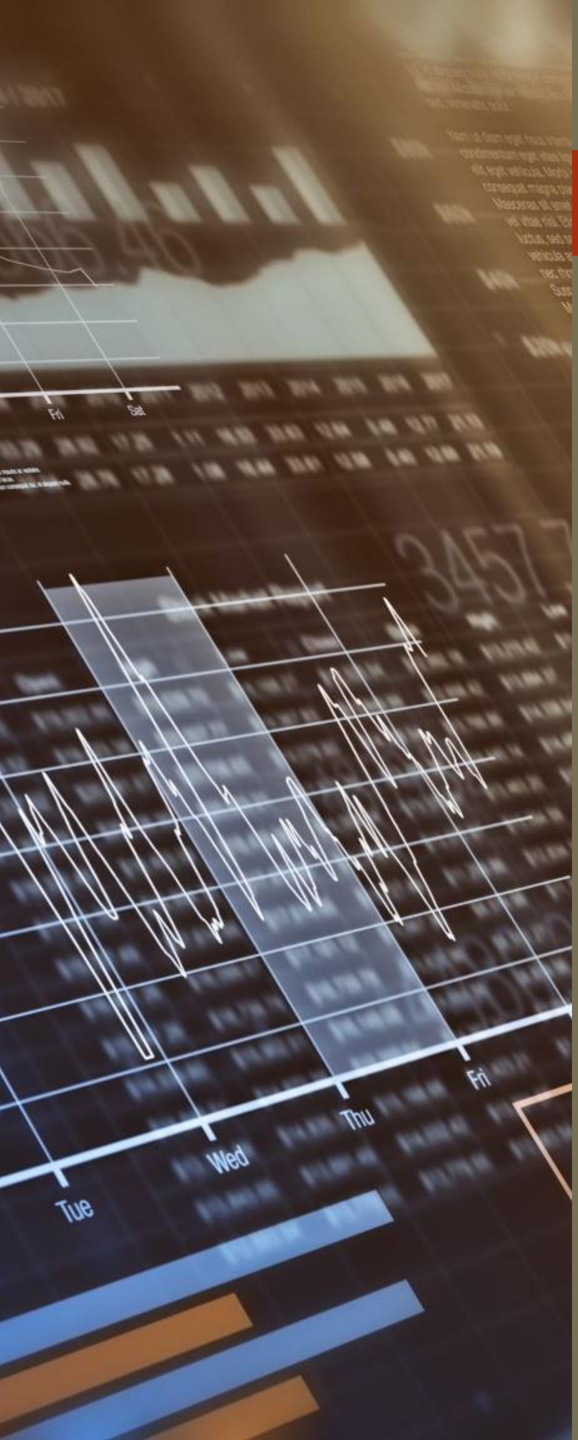


An Image Encryption Algorithm for Medical Images

By :

- ***Ayesha Anjum Shaik, R11800013***
- ***Srikanth Guduru, R11806629***
- ***Lohith Bhargav Doppalapudi, R11786637***
- ***Nikhilesh Reddy Gondesi, R11800323***
- ***Siva Chandu Yadam, R11781983***
- ***Rajani Priya Danda, R11800015***
- ***Ravi Teja Katiki, R11800204***

Why this project is chosen?

- Medical images are considered as one of the most significant and sensitive data in Information systems.
- Sending medical images over the network necessitates the use of a robust encryption algorithm such that it is resistant to cryptographic attacks.
- Telemedicine security includes issues such as
  - ➢Authorization
  - ➢Authentication
  - ➢Accounting
  - ➢Integrity
  - ➢Confidentiality

Introduction :

- Medical image encryption is considered as one of the most predominant fields of cryptographic systems.
- The main purpose of medical image encryption is for the
  - Secure transmission of medical records of patients
  - Ensuring confidentiality and integrity
  - Avoiding changes in medical images that may lead to false diagnosis
  - Persisting from cybersecurity attacks and threats.

Medical Encryption Techniques :

Watermarking :

- The process of hiding the medical image inside a carrier signal
- This is used to ensure the authenticity and integrity of the medical image.

Using Edge Maps :

- Bit plane modification
- Creation of random sequence
- Arrangement process

Adaptive Medical Image Encryption :

- Chaotic logistic maps are used to produce an order of sub keys and the image is encrypted using those sub keys generated by logistic maps.

Medical Encryption Techniques :

Scrambling :

- This changes the understandable format of text to non understandable format in order to avoid illegal viewing of confidential data.
- This process is now automated by the use of scramblers
- Its mainly used for two reasons :
  - To ensure recovery of confidential data
  - To ensure that no data is modified or lost during transmission.

Diffusion :

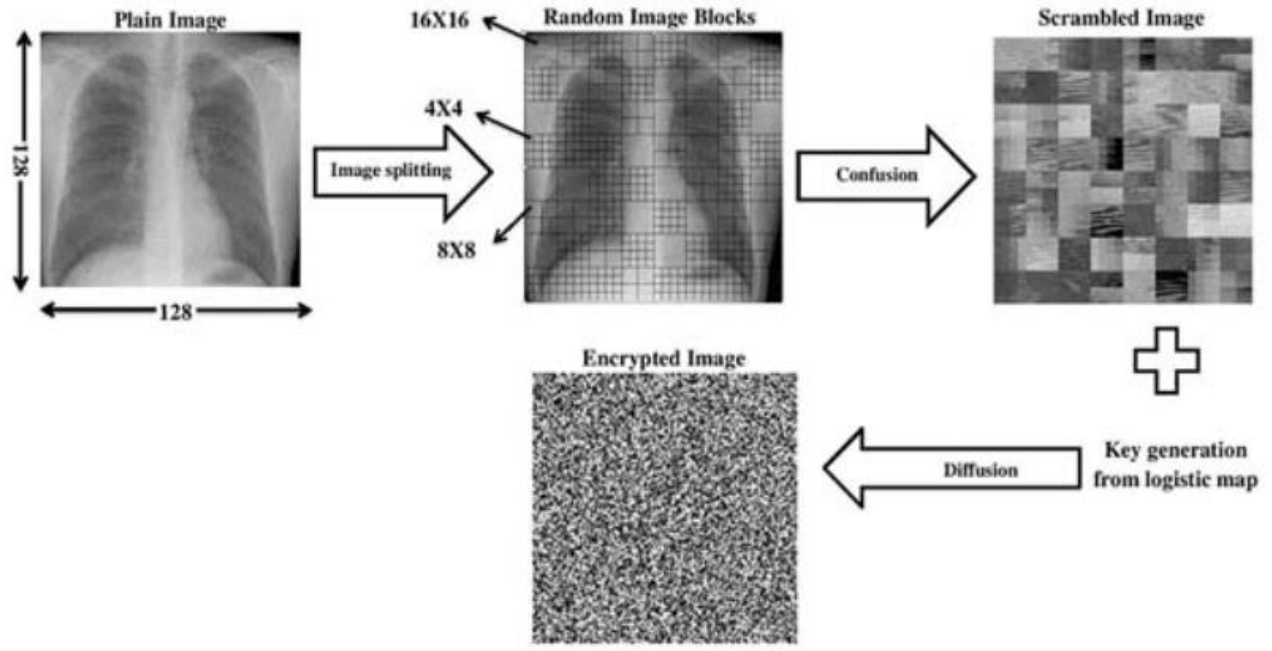
- Process where a single bit change can lead to serious changes in the input text
- It is done using Bitwise-XOR and modulo arithmetic
  - Bitwise-XOR provides higher efficiency in case of hardware platforms
  - Modulo arithmetic provides faster execution speed in case of software platforms

Problem Statement :

- Different algorithms for securing medical images are introduced, yet they may be liable to attacks.
- Main issue : A strong correlation between neighboring pixels characterizes medical images; thus, removing this correlation requires a permutation (scrambling) technique with a higher security level

Our Proposal :

- A new encryption algorithm for encrypting both grey and color medical images.
- A new image splitting technique based on image blocks introduced.
- The image blocks scrambled using a zigzag pattern, rotation, and random permutation.
- A chaotic logistic map generates a key to diffuse the scrambled image.



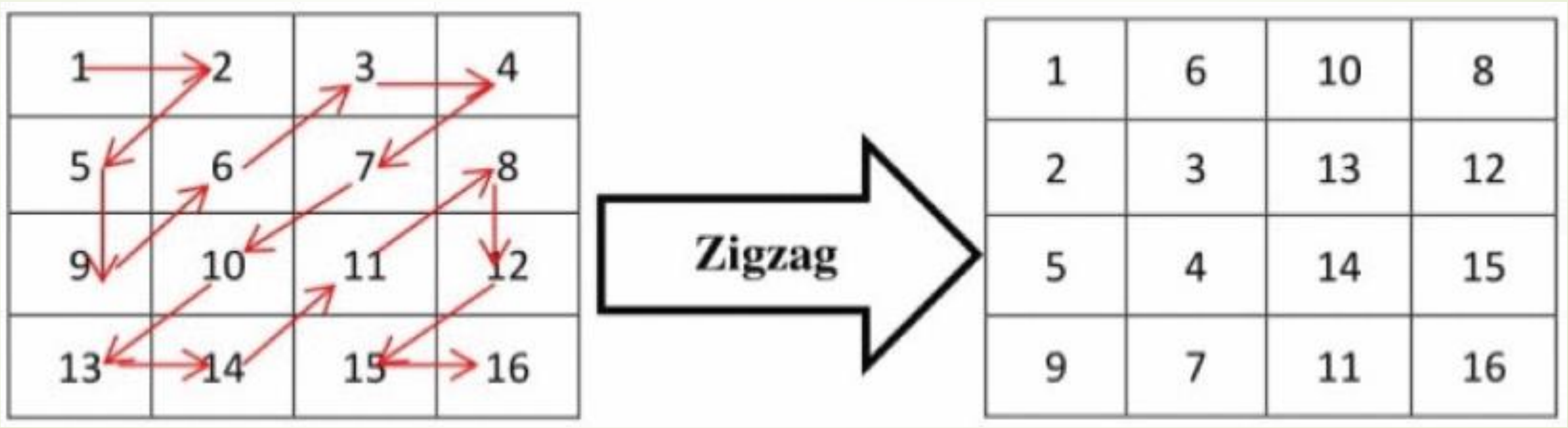
Medical image encryption block diagram.

Step 1 : Plain Image Splitting

- The plain image is divided into non-overlapping blocks of the same size. Our algorithm is appropriate for different block sizes (i.e., 16, 32, and 64), and the user can select the block size.
- Then, each block is either sub-divided into sub-blocks with equal sizes or remains without splitting.
- The sub-blocks in each block are chosen depending on a random number generated for each block.

Step 2 : Confusion

- The zigzag pattern is applied to both undivided blocks and sub-blocks.
- Both undivided blocks and sub-blocks rotated by 90°.
- Random vector r generated where its size is equal to the number of blocks in the plain image.
- Random permutation between blocks based on the vector r is applied to get the scrambled image.



Step 3 : Key Generation

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

The key used in the diffusion process is generated from a logistic map. The logistic map is defined by:

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

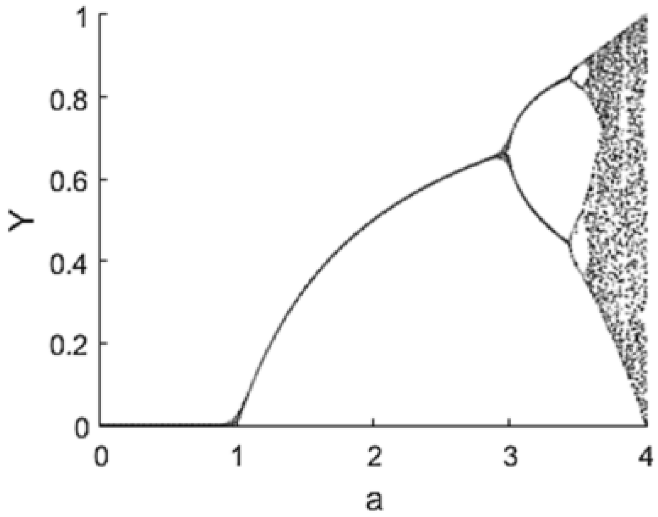
where a is the control parameter with range $0<a\leq4$

$Y0$ is the initial value

Yn is the output sequence with $0<Yn<1$

The map is chaotic when $a\in[3.57,4]$.

Where M and N, refer to the number of rows and columns in the plain image



Step 4 : Diffusion

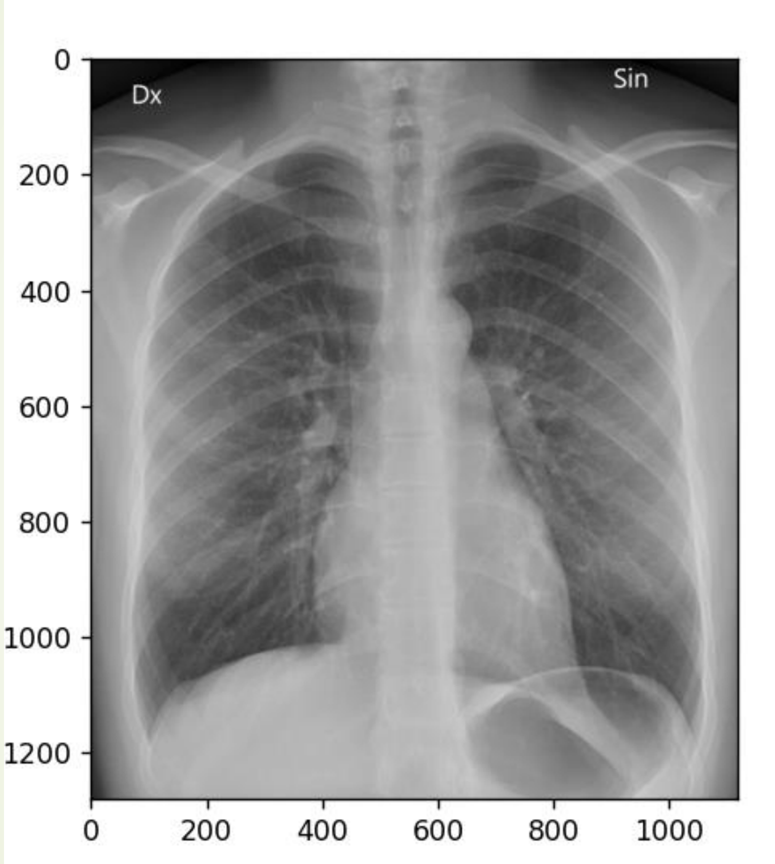
- In the diffusion process, image pixel values are changed, and then a noise image is generated.
- Bit-wise Exclusive OR operation between the key K and the scrambled image vector is performed to obtain the encrypted image.

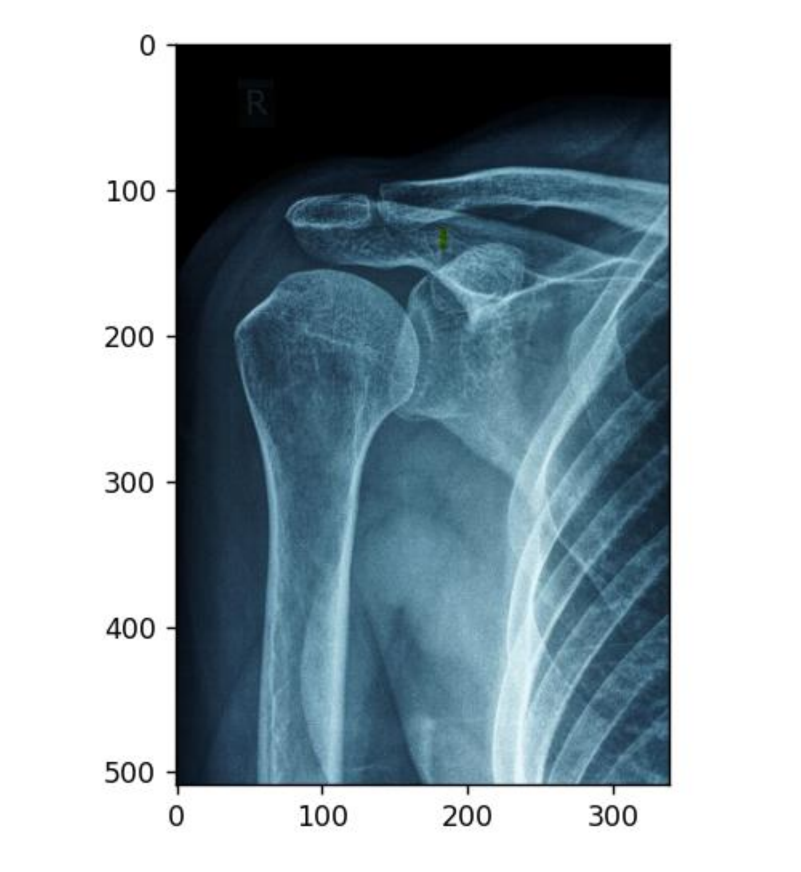
Decryption :

With the original key and by inverting the encryption stages, we can retrieve the plain image. The decryption process is described as follows:

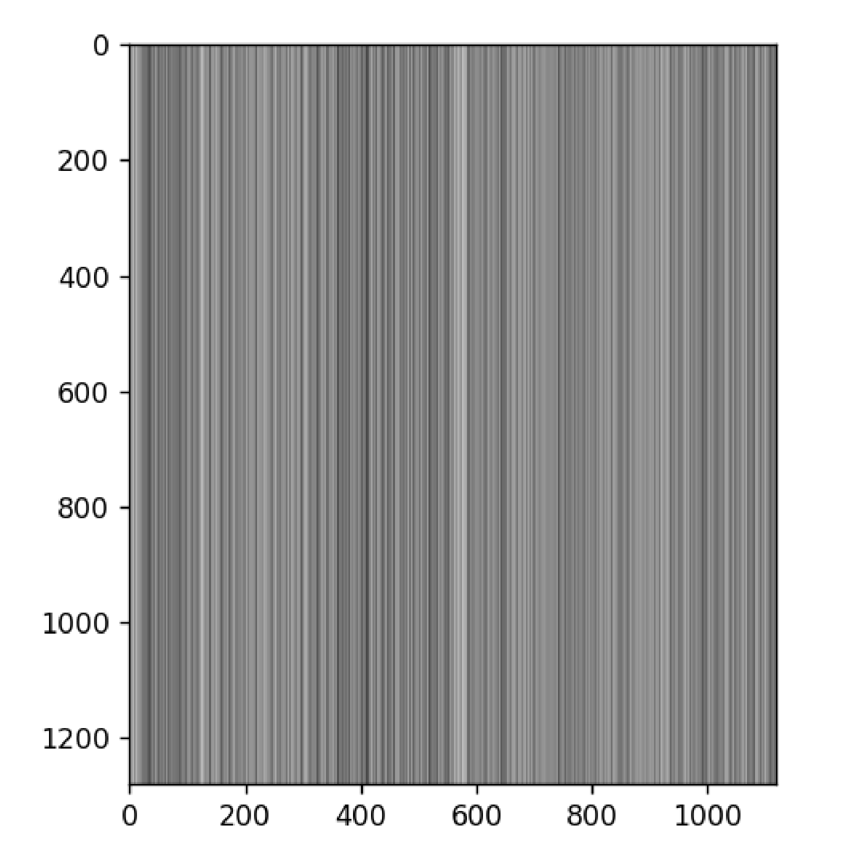
- Bit-wise exclusive OR operation between the key K and the encrypted image vector is applied to get the scrambled image.
- Return each block to its original position using vector r .
- The inverse operation of rotation and the zigzag pattern, respectively, are applied to both undivided blocks and sub-blocks.

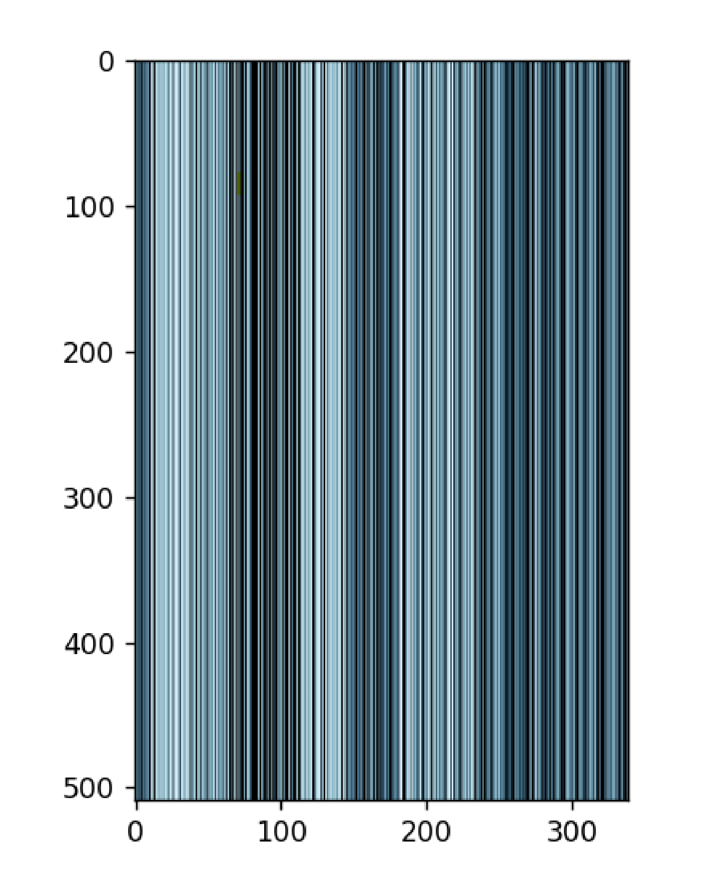
Grey and Color Plain Images Input



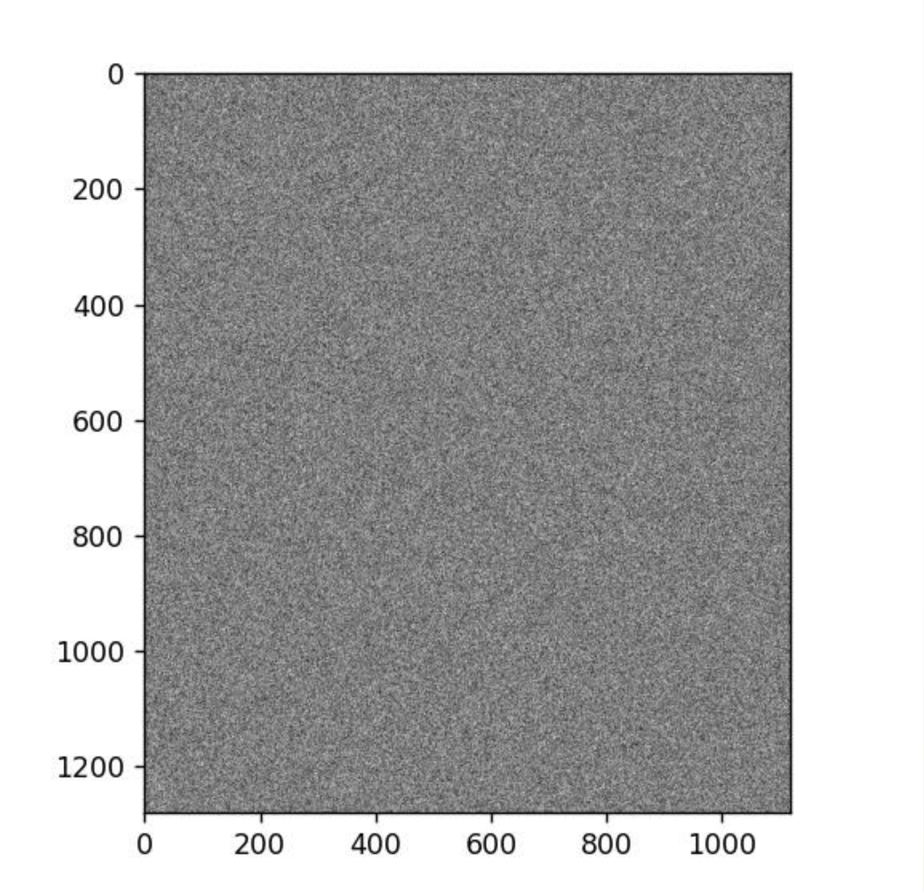


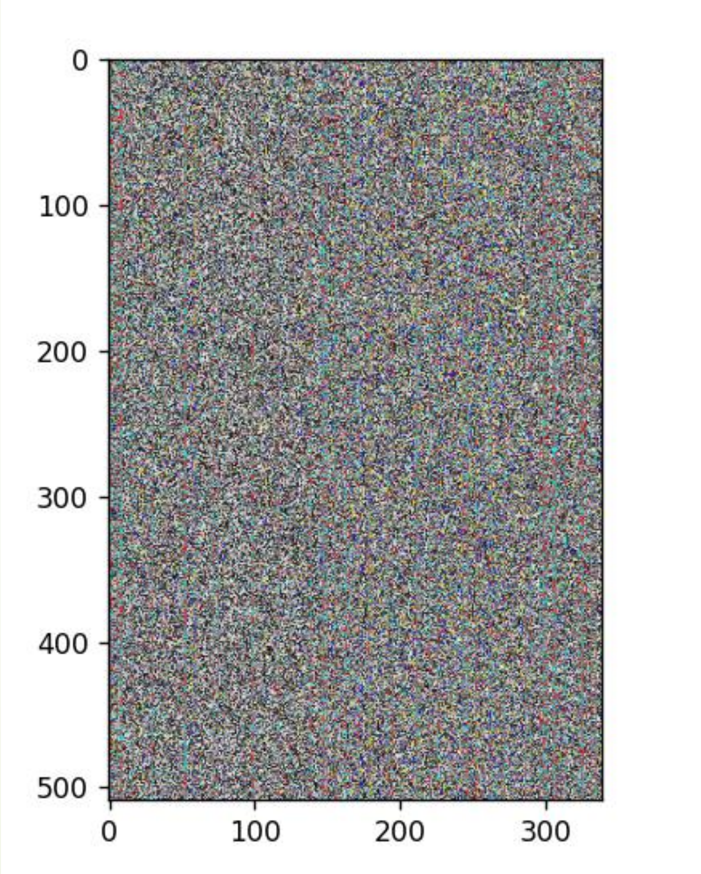
Grey and Color Shuffled Images



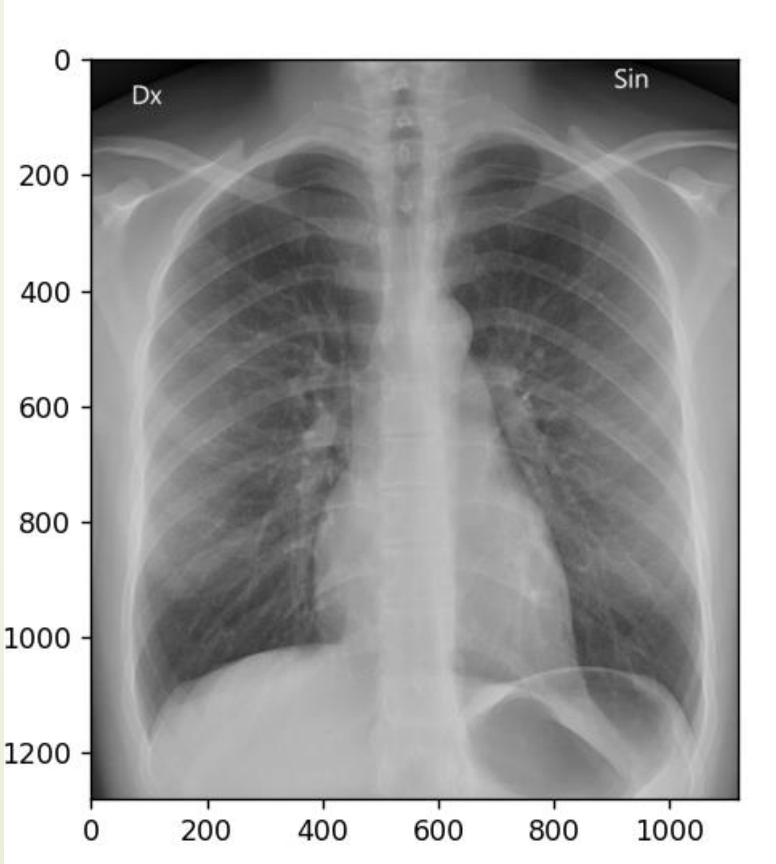


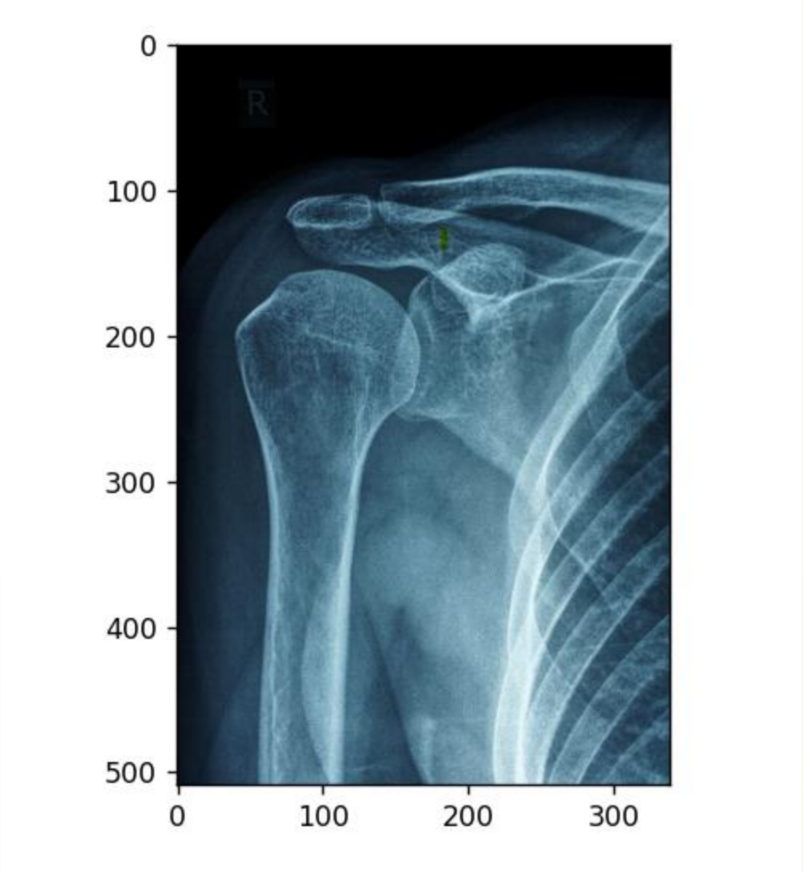
Grey and Color Encrypted Images





Grey and Color Images After Decryption





Testing Result Analysis of Color Medical Image:

- Color images contain more information than grey ones as each pixel in a color image has three values (Red, Green, and Blue).
- So, encrypting color images could be done by separating the image into three channels (R, G, and B) then using the algorithm to encrypt each channel independently.

Testing Result Analysis of Time Complexity :

- We estimate the time complexity in each step of the encryption process to evaluate our proposed algorithm's total time complexity.
- Assume that the plain image is with size $M \times N$, and the block size h=2n where n=4 .
- The time complexity for the plain image splitting and confusion stages is $O((M \times N)/h2)$.
- For the key generation stage and the diffusion stage, the time complexity is $O(M \times N)$. Therefore, the total time complexity of our proposed algorithm is $O(M \times N)$.

Conclusion :

- A new algorithm is introduced for encrypting medical images based on image blocks and chaos.
- The proposed algorithm’s image encryption performance tested using
  - Entropy
  - Histogram
  - Correlation coefficient
  - Differential attack
  - Keyspace
  - Key sensitivity
- Results showed that the proposed algorithm is efficient in encrypting both grey and color medical images.
- Our algorithm compared to other recent encryption algorithms, and the results confirm that the proposed algorithm has good characteristics in encrypting both grey and color medical images.

References :

- https://ieeexplore.ieee.org/document/9366688/references#references

  A New Image Encryption Algorithm for Grey and Color Medical Images, IEEE, 2017
- https://sci-hub.hkvisa.net/10.1016/j.ijleo.2017.08.028

  D. S. Laiphrakpam and M. S. Khumanthem, "Medical image encryption based on improved ElGamal encryption technique", Optik, vol. 147, pp. 88-102, Oct. 2017.
- https://sci-hub.hkvisa.net/10.1016/j.sigpro.2017.10.004

  Z. Hua, S. Yi and Y. Zhou, "Medical image encryption using high-speed scrambling and pixel adaptive diffusion", Signal Process., vol. 144, pp. 134-144, Mar. 2018.
- https://sci-hub.hkvisa.net/10.1016/j.optlaseng.2020.106026

  M. Chen, G. Ma, C. Tang and Z. Lei, "Generalized optical encryption framework based on shearlets for medical image", Opt. Lasers Eng., vol. 128, May 2020.
- https://sci-hub.hkvisa.net/10.1016/j.sigpro.2016.10.003

  W. Cao, Y. Zhou, C. L. P. Chen and L. Xia, "Medical image encryption using edge maps", Signal Process., vol. 132, pp. 96-109, Mar. 2017.
- https://sci-hub.hkvisa.net/https://ieeexplore.ieee.org/document/8782432

  A Survey on the Techniques of Medical Image Encryption, V. Pavithra, C. Jeyamala, 2019.

THANK YOU