A New Image Encryption Algorithm for Grey and Color Medical Images

Ayesha Anjum Shaik – Srikanth Guduru – Lohith Bhargav Doppalapudi – Nikhilesh Reddy Gondesi – Siva Chandu Yadam - Rajani Priya Danda – Ravi Teja Katiki

Table Of Contents:

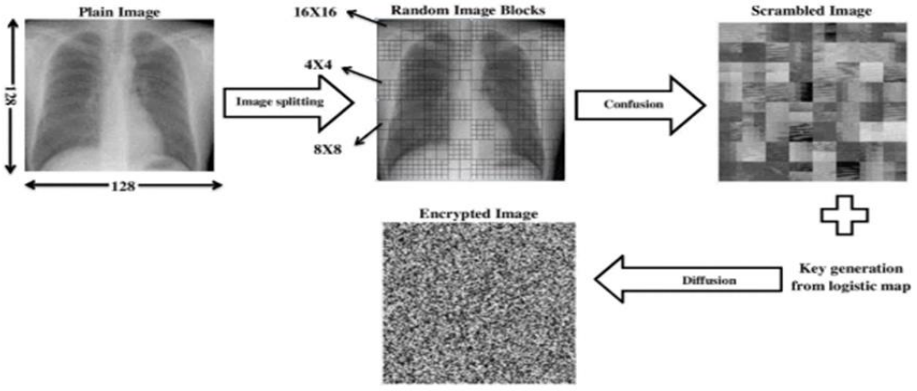
1. *Summary*
2. *The Proposed Algorithm*
    a) *Plain Image Splitting*
    b) *Confusion*
    c) *Key Generation*
    d) *Diffusion*
3. *Output*
4. *Time Complexity, Future Works*
5. *Conclusion*
6. *References*
7. *FAQ*

Presentation Date : Apr 25,2022

Summary: When the medical images are transmitted through the network, they need a high level of protection. The most efficient technique for securing medical images is encryption in which confusion and diffusion are the two main steps. This topic presents "A New Image Encryption Algorithm for Grey and Color Medical Images". Firstly, the plain image is divided into blocks and sub-blocks using a new image splitting technique. In the second step, the pixels arrangement is changed in the blocks and sub-blocks using a zigzag pattern, rotation at a 90-degree angle, and random permutation between blocks. In the third step, a key is generated from the logistic map, where the map's initial condition depends on the plain image. Finally, the image pixel values are changed using the secret key. 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. The three security objectives for the security of information systems namely confidentiality, integrity, and availability. Confidentiality is the most important aspect that need to be taken much care for the secure storage and transmission of medical images.

2.The Proposed Algorithm

The algorithm for encrypting medical images consists of four steps

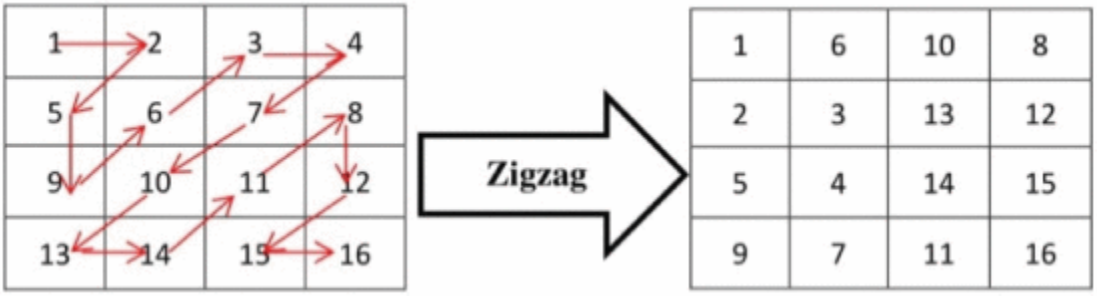


a) Plain Image Splitting

The plain image is divided into different block sizes (i.e., 16, 32, and 64), and the user can select the block size. 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.

b) Confusion: It is the process of changing pixels arrangement in the image.

- 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.

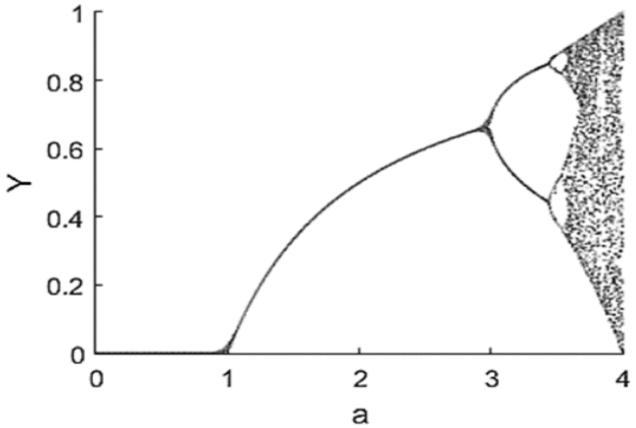


c) Key Generation

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, and Y_n is the output sequence with $0<Y_n<1$. The map is chaotic when $a\in [3.57,4]$. The below shows the bifurcation diagram of the logistic map. The key generation steps are defined as follows:

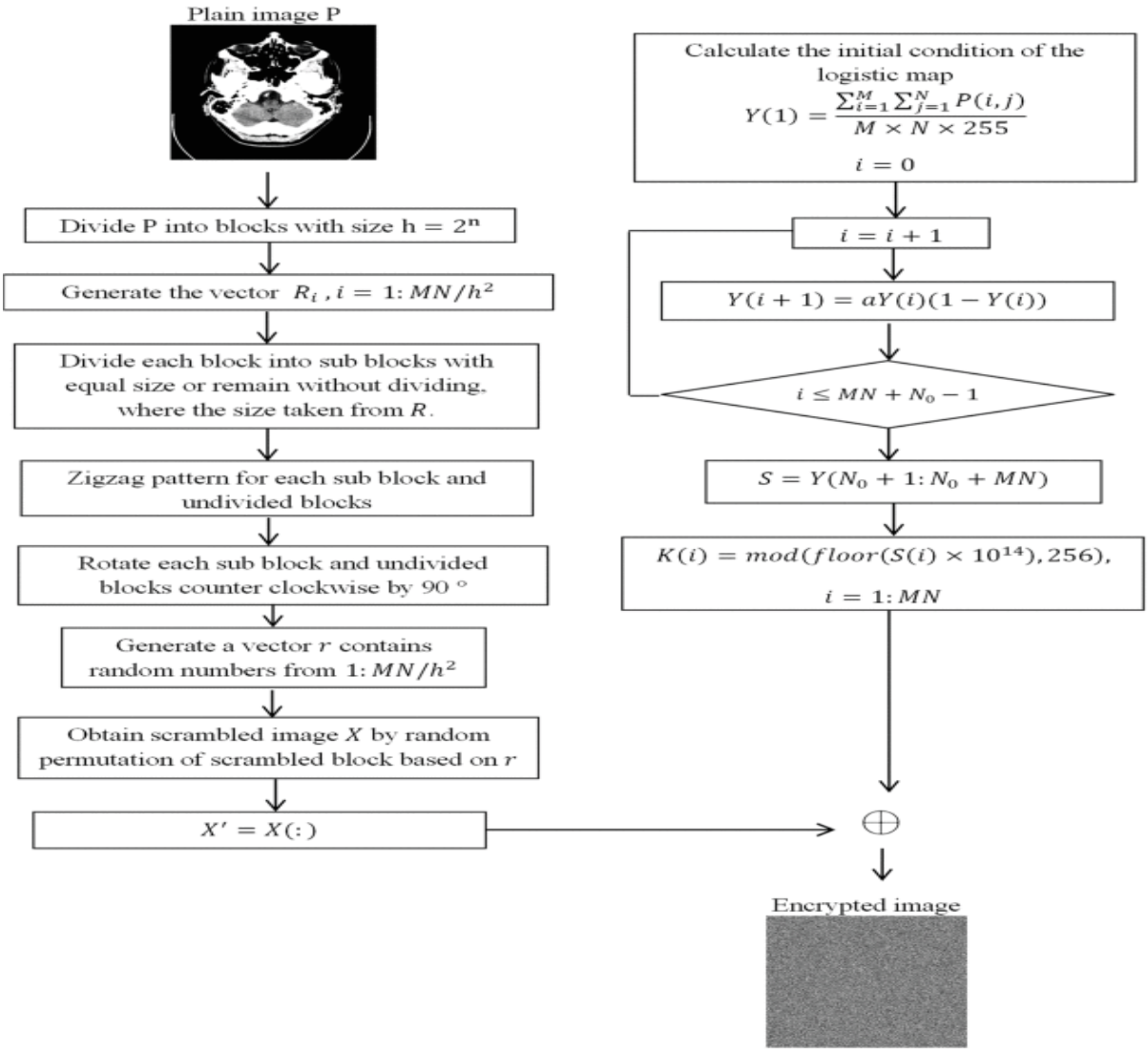
- Calculate the initial value of the logistic map that depends on the plain image P by using below equation: $Y_0=\sum M_i=1\sum j=1NP(i,j)M\times N\times 255(2)$
- The numbers, M and N, refer to the number of rows and columns in the plain image, respectively.
- Iterate the chaotic map N_0+MN times, and then skip the first N_0 elements to get a new sequence S with size MN.
- We calculate the key using the below formula:



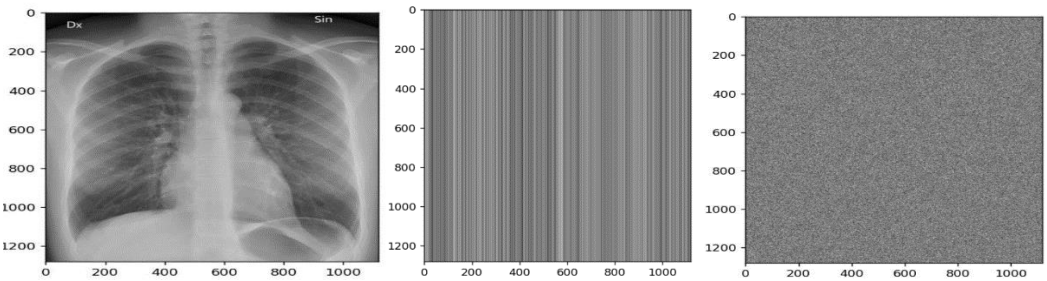
$K(i)=mod(floor(S(i)\times1014),256),i=1:MN(3)$

d) Diffusion

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.



3) Output



4) Time Complexity

Let the plain image is with size M×N, and the block size h=2n where n=4. The time complexity for the plain image splitting and confusion stages is O((M×N)/h2). For the key generation stage and the diffusion stage, the time complexity is O(M×N). Therefore, the total time complexity of our proposed algorithm is O(M×N).

Future Works : Certain ideas we aim to implement in the future are as follows :

- To extend this method to video encryption since videos, essentially, are a collection of continuous frames, i.e. images.
- For Dynamic Encryption, the key used for the image encryption can be made dynamic but we will need to implement a process to store the repeatedly changing key to ease the process of decryption.
- To test the proposed algorithm using brute force attacks, AI-based attacks and so on.
- To implement higher factor authentication

5)Conclusion: The proposed algorithm's image encryption performance tested using entropy, histogram, correlation coefficient, differential attack, key space, and 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.

6) 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.

7)FAQ

- How AES is better than Medical Encryption Algorithm?
  A) The experimental results shows that the AES algorithm presents better security performance but slightly slower in terms of the encryption running speed, this allows us to recommend it for selective image encryption, unfortunately, it is noted that the logistic map shows some periodic windows that make it vulnerable. However, due to the computational cost, and the simplicity of implementation this map is a good alternative for image encryption in real time communication applications with the condition to combine it with other chaotic maps or other encryption techniques.
- Describe time complexity?
  A) The time complexity for the plain image splitting and confusion stages is O((M×N)/h2). For the key generation stage and the diffusion stage, the time complexity is O(M×N). Therefore, the total time complexity of our proposed algorithm is O(M×N).
- Explain Key Generation?
  A) Check page 2 for clear explanation of key generation.
- How Key generation is bearable to cryptanalysis?
  A) The main reason why we used chaotic maps for key generation is, in so many chaotic cryptosystems, the high dependency of the dynamics of chaotic maps on an external value or set of values and the initial conditions of the system which results in the dependency of the cryptosystem on the secret key, also having a critical point independent to the value of control parameters, whereas the statistical complexity decrease as the control parameters increase.
- How can receiver decrypt the image? How receiver works on Key and techniques like zigzag pattern, rotation, random permutation?
  A) In the receiving end, the receiver with encryption key can decrypt the image by using the following steps.
    - 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.