**International Journal of Research Publication and Reviews**

Journal homepage: www.ijrpr.com ISSN 2582-7421

# A Novel Image Encryption Algorithm for Grey and Color Medical Image

***V. Nagamani[1], P. Naga Divya[2], N. Sangeetha[3], K. Pavani[4], S. Jahnavi Sameera[5]***

[1]Assistant Professor ECE Department, Santhiram Engineering College, Nandyal, AP, India.
[2,3,4,5] Student, ECE Department, Santhiram engineering college, Nandyal, AP, India.

**ABSTRACT**

Recently, diagnosing diseases using medical images became 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. Confusion and diffusion are the two main steps used in encryption algorithms. This paper presents a new encryption algorithm for encrypting both grey and color medical images. A new image splitting technique based on image blocks introduced then, the image blocks are scrambled using a zigzag pattern, rotation, and random permutation. Then, a chaotic logistic map generates a key to diffuse the scrambled image. The efficiency of our proposed method in encrypting medical images is evaluated using security analysis. The security is tested in histogram differential attacks, PSNR. The achieved results show a high-performance security level reached by successful encryption of both grey and color medical images. A comparison with various encryption methods is performed. The proposed encryption algorithm out performed the recent existing encryption methods in encrypting medical image.

**Keywords:** Image Smoothing – wavelet Transform – Bi-convex set.

## 1. INTRODUCTION

Cryptography is the study of securing communications from outside observers. Encryption algorithms take original message, or plaintext, and converts it into ciphertext, which is not understandable. The key allows the user to Decrypt the message, thus ensuring on they can read the message. The strength of the randomness of an encryption is also studied, which makes it harder for anyone to guess the key or input of the algorithm. Cryptography is how we can achieve more secure and robust connections to elevate our privacy. Advancements in cryptography makes it harder to break encryptions so that encrypted files, folders, or network connections are only accessible to authorized users.

Cryptography focuses on four different objectives:

**1.Confidentiality**: Confidentiality ensures that only the intended recipient can decrypt the message and read its contents.

**2.Non-repudiation**: Non-repudiation means the sender of the message cannot backtrack in the future and deny their reasons for sending or creating the message.

**3.Integrity**: Integrity focuses on the ability to be certain that the information contained within the message cannot be modified while in storage or transit.

**4.Authenticity**: Authenticity ensures the sender and recipient can verify each other's identities and the destination of the message.

These objectives help ensure a secure and authentic transfer of information.

## 2. METHODOLOGY

The system proposes a new RDH scheme using the controlled contrast enhancement (CCE) and Haar integer wavelet transform (IWT). There are two main parts in the message embedding process, including data embedding with CCE in spatial domain and more data embedding in Haar IWT domain. The data extraction and image recovery are the reverse procedure of data embedding process. Preprocessing image is basic step in all the image processing process. A pre processing needs to be used to prevent the overflow/underflow. The Haar IWT of an image can be realized by two dimensional transform. The approximation sub band is highly sensitive to coefficient changes, thus the coefficient modifications on sub band for embedding bits can lead to obvious influence on image contrast which can produce severe visual distortion. The horizontal subband, diagonal sub band and vertical sub band are detail subbands where coefficients accord with Laplacian like distribution. The coefficient changes on horizontal subband, diagonal subband and vertical subband only have very small effect on image contrast. A proper image contrast enhancement is achieved during the data embedding into the image in

spatial domain by monitoring the contrast enhancement indicator. Then it is shown that the modification of the detail subband coefficients in IWT domain only produces very small contrast change. This leads to embedding more data into the detail subbands without lowering the visual quality significantly. More message bits are embedded into detail subbands, using the companding echnique. For the restoration of original coefficient, the length of location map, the companding error, the threshold and the compressed location map, as side information, should be embedded into the cover image along with the message bits.

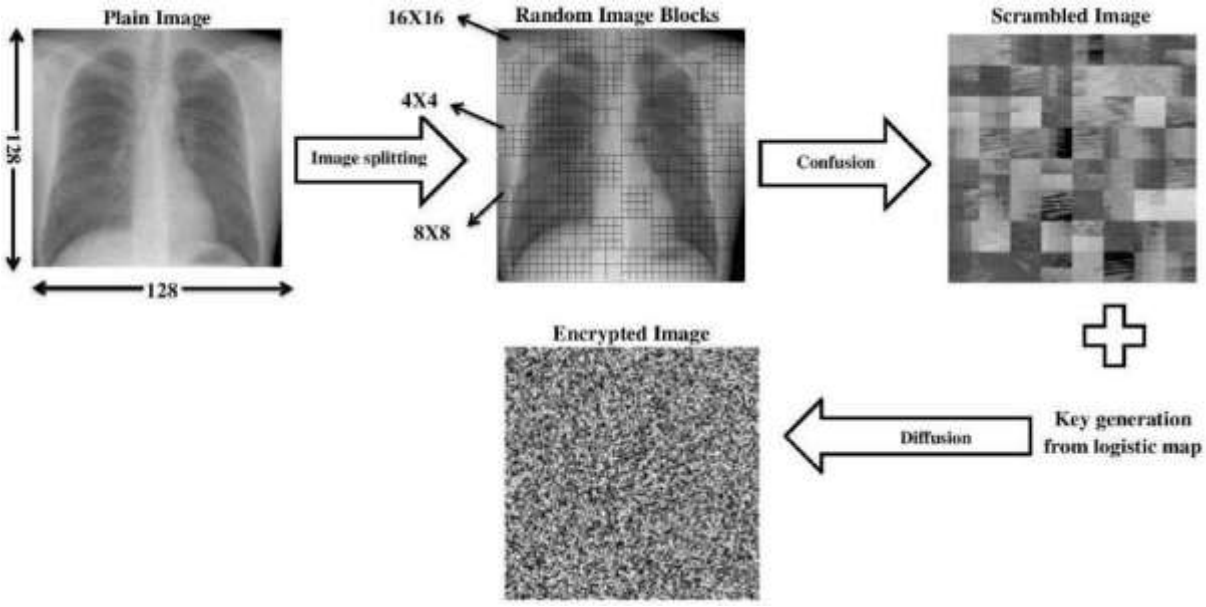


Fig1:- Medical image encryption block diagram

The proposed chaos-based cryptosystem for color images consists of the following four parts: i) an image division-shuffling process, ii) a key streams generation process, iii) an image permutation process and iv) an image diffusion

process. The flowchart of the image encryption procedure using the proposed scheme is displayed . Firstly, the plain- image is divided into four sub-images, and then these blocks are shuffled to obtain a disordered image. This process can enhance the resistance of the cipher-image against plaintext attack. Secondly, a 280- bit external secret key is used to generate initial conditions and parameters of the CML and the fractional-order chaotic system. The key streams can be generated by using the obtained initial conditions and parameters to iterate the CML and the

fractional-order chaotic system. Thirdly, the positions of the image pixels are permuted by the pseudo- random key stream generated from the CML. In the last stage, the pixel values are modified by the pseudo-random key stream generated from the fractional-order chaotic system. After this, the cipher-image is finally achieved

## 3. MODELING AND ANALYSIS

The proposed algorithm's main steps for securing medical images in detail. In the first step, the plain image is encrypted and converted into an unreadable image. Then, to recover the plain image, we apply the decryption step.

### *1. ENCRYPTION*

Here, our algorithm for encrypting medical images consists of four stages. In the first stage, we perform image splitting. Confusion (scrambling) is performed in the second stage. The third stage presents key generation based on a logistic map.The final stage presents the diffusion process.

### *1.1 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.

### *1.2. 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:

Confusion is the process of changing pixels' arrangement in the image.

In our algorithm, confusion is performed for blocks and sub- blocks as follows:

The zigzag pattern is applied to both undivided blocks and sub- blocks, as described:

1. Both undivided blocks and sub-blocks rotated by 90◦.
2. Random vector generated where its size is equal to the number of blocks in the plain image.
3. Random permutation between blocks based on the vector r is applied to get the scrambled image.

***2.KEY GENERATION***

The key used in the diffusion process is generated from a logistic map. The logistic map is defined by: Yn+1 = aYn (1 − Yn) (1) where a is the control parameter with range $0 < a \leq 4$, Y0 is the initial value, and Yn is the output sequence with $0 < Yn < 1$. The map is chaotic when $a \in [3.57, 4]$. Figure 3 shows the 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:

Y0 = I i=1 to M j=1 to N P(il, j) /M × N × 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) mod ( floor( S (i) × 1014) , 256) , i = 1 : MN

***3.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. Detailed encryption steps are presented in Algorithm.

## 4. RESULTS

Fig:8.1 Input grey image

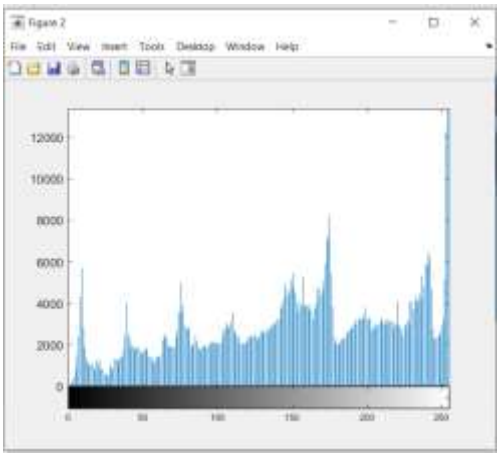


Fig:8.2 Histogram of Input grey image


Fig: 8.3 Enter key value

Fig: 8.4 Encrypted grey image

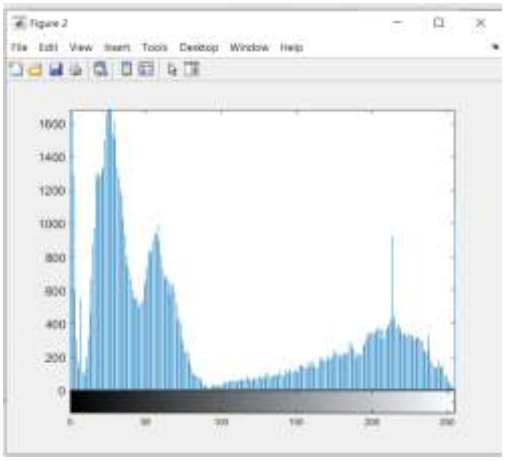


Fig: 8.8 Histogram of input colorimage

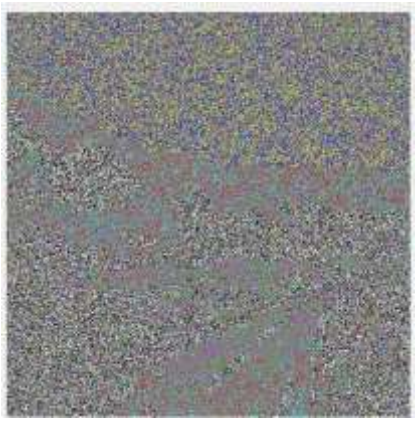

Fig: 8.10 Encrypted color image

## 5. Conclusion

The proposed algorithm's image encryption performance tested using histogram differential attacks, PSNR 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. APPLICATIONS:

- Internet communication
- Medical imaging
- Telemedicine
- Military communication
- Multimedia systems

### 7. References

[1]. P. Bas and T. Furon, "A new measure of watermarking security:The effective key length," I E EETr a n s. I n f. F o re n s i c s Se c u r., vol. 8, no. 1, pp. 1306–1317, 2013.

[2]. J. Li, X. Li, B. Yang, and X. Sun, "Segmentation-based image copy move forgery detection scheme," I E EETra n s. Inf. Forensics Secure., vol. 10, no. 3, pp. 507–518, 2015.

[3]. J. Tian, "Reversible data embedding using a difference expansion," I E EETr a n s . Circuits syst. Video Technol., vol. 13, no. 8, pp. 890–896, 2003.

[4]. Q. Gu and T. Gao, "A novel reversible robust watermarking algorithm based on chaotic system," Dig. Signal Process ., vol. 23,no.5,pp.213–217, 2013.

[5]. H. C. Huang, F. C. Chang, and W. C. Fang, "Reversible data hiding with histogram-based difference expansion for QR code applications," I E EETr a ns . Consumer Electron ., vol. 57, no. 2, pp. 779– 787, 2011.

[6]. Z. C. Ni, Y. Q. Shi, N. Ansari, and W.Su, "Reversible data hiding," I E EETr a n s . Circuits Syst . Video Technol ., vol. 16, no. 3, pp. 354–362, 2006.

[7]. G. Coatrieux, W. Pan, F. Cuppens, and C. Roux, "Reversible watermarking based on invariant image classification and dynamic histogram shifting," IEEETr a ns . I n f . Forensics Secure., vol. 8, no. 1, pp. 111–120, 2013.