DOI : https://doi.org/10.56452/7-80101

ISSN: 0974-5823 Vol. 7 No. 01 (January, 2022)

International Journal of Mechanical Engineering

A New Transformation for Chaotic Medical Image Encryption based on ACM

Karthika A[1], Dr. D. Kiruba Jothi[2]

[1]Research Scholar, Registration Number: 20211252272004, Department of Information Technology, Sri Ram Nallamani Yadava College of Arts and Science, Tenkasi, Manonmanaiam Sundaranar University, Tirunelveli, Tamilnadu, India.

[2]Research Supervisor, Department of Information Technology, Sri Ram Nallamani Yadava College of Arts and Science, Manonmanaiam Sundaranar University, Tirunelveli, Tamilnadu, India.

Abstract: Medical Data security is concerned with maintaining the secrecy, reliability and accessibility of data. The main objective of Medica information security is to protect information and information system from unauthorized access, revelation, disruption, alteration, annihilation and use. This paper uses method for information embedding an Arnold's transform is applied multiple iterations with different intervals to ensure security. The system is tested and validated Medical Image Encryption using Arnold Cat Map Transformation. However, this paper proposed to generates a larger set of Transformation matrices. Thus, no one easily estimating the Transformation Matrix used for scrambling. Because the modified Arnold Cat Map transform matrix is no fixed structure matrix, so difficult to find the appropriate transformation matrix. The quality of the shuffling process and strength of this proposed algorithm is also tested using different medical images.

Keywords: *- Arnold's Cat Map, Medical Image Security, Transformation matrix*

Introduction

With the rapid advancement of multimedia technology on the Internet, vital information increasingly becomes available in the form of images and videos, with security becoming a serious issue. Images can be secured by means of encryption. Owing to certain intrinsic characteristics of images like high data redundancy, strong correlation among neighboring pixels and bulk data capacity, however, image encryption differs from that of text. Consequently, algorithms suitable for textual data may not be as appropriate for images. Despite the sizeable number of image encryption algorithms in existence, image scrambling is a common method employed to encrypt image data so as to hide content from unauthorized users. Chaotic maps are useful in ensuring the security of digital images by means of scrambling, because they are easy to generate but deterministic and difficult to predict. The base of these maps is a combination of substitution and diffusion [1]. In the substitution stage, the chaotic map shuffles image pixels and in the diffusion stage, pixel values are altered. The Arnold transform, a chaotic map, is an effective image scrambling tool used widely in digital image scrambling. The transform is used in watermarking algorithms to scramble watermark images [2], so as to enhance their privacy and robustness. An image encryption scheme presented in [3] combines shuffling positions and changing the gray values of the image pixels to set off confusion in the relationship between the cipher image and the plain image. Here, the Arnold cat map shuffles the positions of the image pixels in the spatial domain. But the author of [6] found the scheme presented in [5] unable to resist chosen-plaintext attacks and known-plaintext attacks, and based on the scheme in [5], proposed a modified scheme in [6] which can resist both types of attacks. The Arnold transforms augments security [7] and scrambles image slices to enhance security [8] so that an authenticated receiver with an appropriate key alone can descramble the images. The authors of [9] have proposed a fragile watermarking algorithm in which the Arnold cat map scrambles the original image before the watermark is embedded into it. Encryption schemes are proposed, based on the Arnold transform, along with other chaotic maps such as the Henon [10] and quantum [11] chaotic maps. A cryptosystem for RGB images is designed in [12] with the affine hill cipher (AHC) over the SLn(Fq) and Mn(Fq) domains, along with the Arnold transform. Based on the generalized Arnold transform, an image zero-watermarking scheme with spread spectrum and de-spreading (SSD) techniques is presented in [13]. An optical multiple-color image security system based on the generalized Arnold map in the gyrator transform domain is investigated by [14]. In [1] a double image encryption algorithm is designed by using Arnold transform and discrete angular transform. The Arnold transform is used to obtain the embedding positions of the watermark in [6]. A quantum realization of the generalized Arnold transform is designed in [7]. In most cases, as exemplified in the literature above, the Arnold transform serves its basic purpose, that of scrambling image pixels.

The result is utilized for various purposes like Medical Image enhancing security. A new transformation method proposed in this paper based on the Arnold cat map and mainly deals with increasing the key space by much more than the one offered by the Arnold transform. Also, the proposed transformation shuffles the pixels better at the earliest iterations than the Arnold, thus rendering the proposed transformation eminently appropriate for real-time applications. The rest of this paper is organized as follows. Section 2 describes the proposed new transformation algorithm - Arnold transformation for an image. Experimental results and analysis outputs are detailed in Section 3. Finally, the conclusion on the findings is presented in Section 4.

Proposed Algorithm

Read the input medical image of .jpg or (.jpeg,.png,.tiff,.bmp) any format is chosen for the process of encryption. Pixel extraction is done of the input medical image by taking the image dimension. i.e. Height and Width of the original image. Pixel shuffling or transformation of the input medical image done by Arnold Cat Map encryption and decryption equations. During execution time the secret key values also used. The secret key values are two parameters ‘p’ ,’q’, number of iterations ‘R’ and the size of the original medical image ‘N'. Iterations are done between the input pixel values and the key values are generated from each iteration. Here the iteration values are chosen as random manner and cannot be identify easily by attackers and unauthorized persons. Cipher image or encrypted image is successfully generated. Encrypted image cannot be identified without knowing the value of iteration and also the secret key values, because it performing the iterations for n in the pixel image. Cryptography is the process, to keep the medical images, data and patient information more confidential based on the Arnold cat map transformation of encryption and decryption. In this algorithm to protect the medical data from the attackers, unauthorized members get an opportunity to reuse, retrieve, disturb the medical images.

- ***Arnold Cat Map Transformation***

Arnold cat map is a two-dimensional transformation map it is used to change or shuffle the pixel positions of the input medical image without loss of any information. After applying the transformation, the pixels are rearranged. When the transformations are repeated for a particular time period, the input medical image will reappear [6-9] .

The pixel of the image denoted by Z=$\{(a,b)|a,b = 0,1,2,\ldots..N-1\}$. The two-dimensional cat map transformation formula is given below

$$\begin{bmatrix} a' \\ b' \end{bmatrix} = A \begin{bmatrix} a \\ b \end{bmatrix} (\bmod n) \quad 1)$$

$$\begin{bmatrix} 1 & p \\ q & pq+1 \end{bmatrix} \begin{bmatrix} a \\ b \end{bmatrix} \bmod(n) \quad (2)$$

Where p and q are positive integers, the determinant (A) = 1, (a, b) is the original pixel position and the new pixel position denoted as (a ', b'). R should be represented as number of iterations. R is a random number; it contains all the values of the same pixel of the original input medical image. Number of iterations 'R' fully depending upon the parameter values of 'p','q' and the size of the original medical image 'N'. Here the secret keys are represented as the two parameters 'p' and 'q' then the number of iterations 'R' and the size of the input image 'N'. By using these secret keys to generate different Arnold Cat map transformation. Without knowing the iteration or secret key values cannot to regenerate the original image. Figure 1 shows the flow chart for Image encryption and decryption using Arnold cat map Transformation.

- ***Architecture for ACMT***

Arnold cat map transformation is a cryptographic algorithm used to encrypt the image by using the continuous iterations. The concept of this algorithm [14] is continuously iterating the image so that it becomes a form that is not visible and it should be random, so that the image cannot be identified by the attackers and unauthorized users without knowing the knowledge of secret keys. By using this secret key to shuffle or rearrange the input pixel values to create new random numbers but without loss of any original information from the input medical image. The secret keys are two parameters p and q, size of the original image N and number of iterations. Always the number of iterations R is fully depended upon the values p, q and N.

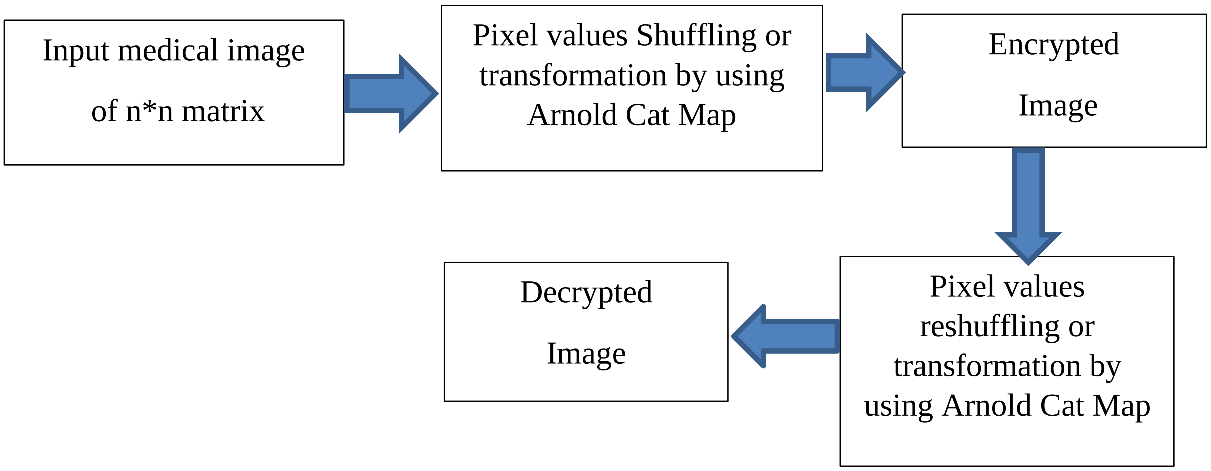

Input medical image of n*n matrix
Pixel values Shuffling or transformation by using Arnold Cat Map
Encrypted Image
Pixel values reshuffling or transformation by using Arnold Cat Map
Decrypted Image

Figure 1. Flow chart for Image encryption and Decryption using Arnold cat Map

Algorithm for ACMT

Step 1: Read the color image of .jpg or (.jpeg,.png,.tiff,.bmp) any format is chosen for the process of encryption.

Step 2: Pixel extraction is done of the input medical image by taking the image dimension. i.e Height and Width of the medical image.

Step 3: Pixel shuffling or transformation of pixels of the input medical image done by using the below Arnold Cat Map encryption and followed by decryption equations.

$$\begin{bmatrix} a_{i+1} \\ b_{i+1} \end{bmatrix} = \begin{bmatrix} 1 & x \\ yy & x+1 \end{bmatrix} \begin{bmatrix} a_i \\ b_i \end{bmatrix} mod(n) \qquad (3)$$

$$\begin{bmatrix} a_i \\ b_i \end{bmatrix} = \begin{bmatrix} 1 & x \\ y & xy+1 \end{bmatrix} \begin{bmatrix} a_{i+1} \\ b_{i+1} \end{bmatrix} mod(n) \qquad (4)$$

Step 4: Generating the secret key values are the two parameters p and q. The number of iterations R and the size of the original medical image N.

Step 5: Iterations are done between the input pixel values and the key values are generated from each iteration. Here the iteration values are chosen as random manner and cannot be identify easily by attackers and unauthorized persons.

Step 6: Cipher image or encrypted image are successfully generated.

Here the below examples show how the iteration steps are work to rearrange or transform the input medical image pixel values by using the secret key values and iterations.

- ***Examples of Arnold Cat Map Transformation:***

For example, here taking the input image pixel value 124 x 124. After fifteen iterations, the pixel in the image returned to its initial position. Here the parameters p and q are 32 and 12 and the size of the image N is 124.

$$\begin{bmatrix}32\\12\end{bmatrix} \text{mod } 124 = \begin{bmatrix}44\\56\end{bmatrix} = \begin{bmatrix}100\\32\end{bmatrix} = \begin{bmatrix}8\\40\end{bmatrix} = \begin{bmatrix}48\\88\end{bmatrix} = \begin{bmatrix}12\\100\end{bmatrix} =$$

$$\begin{bmatrix}112\\88\end{bmatrix} = \begin{bmatrix}76\\64\end{bmatrix} = \begin{bmatrix}116\\32\end{bmatrix} = \begin{bmatrix}24\\32\end{bmatrix} = \begin{bmatrix}56\\88\end{bmatrix} = \begin{bmatrix}104\\108\end{bmatrix}$$

$$= \begin{bmatrix}20\\108\end{bmatrix} = \begin{bmatrix}4\\92\end{bmatrix} = \begin{bmatrix}96\\60\end{bmatrix} = \begin{bmatrix}32\\12\end{bmatrix}$$

Arnold Cat Map transformation implemented for the purpose of security, the security is concerned with keeping the secrecy, reliability and accessibility of medical data in the medical field [12]. The main motivation of the medical data security [10-14] is to protect information and medical data and information system from unauthorized members from outside revelation, disruption alteration, and annihilation. After implementation of this proposed algorithm get fully secure medical image without reducing the original value and information. In this algorithm to protect the medical data from the attackers, unauthorized members get an opportunity to reuse, retrieve, disturb the medical images. Table 1 shows iteration output by using ACM transformation method. Table 2 shows the comparison table for steganography, single LSB substitution and proposed method.

Experimental Results And Analysis

The proposed method is tested and validated over a range of five different standard medical gray scale images of size 512 × 512 and sized 257 KB. Table 2 shows presents the iterations needed for a pixel to shuffle the initial position with Arnold's cat map. Thus, the proposed transfrom is able to offer more key space for encryption. It is also observed that the proposed method shows better scrambling. And also shows the original images considered, the outputs of various iterations are listed.

DOI : https://doi.org/10.56452/7-80101

ISSN: 0974-5823 Vol. 7 No. 01 (January, 2022)

International Journal of Mechanical Engineering

Table 1. Sample output images by Arnold Cat Map Transformation with multiple iterations in increasing

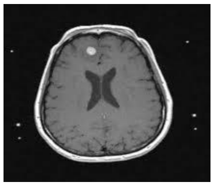
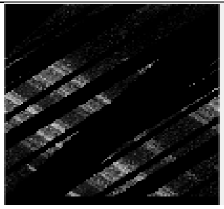
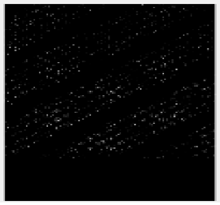
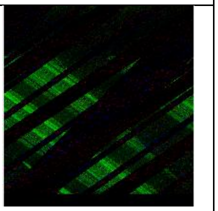
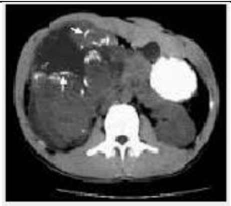
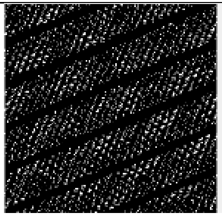
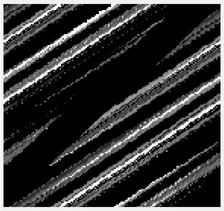
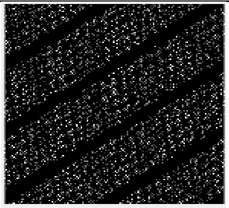
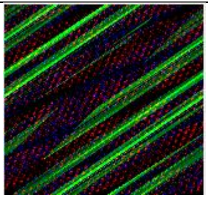
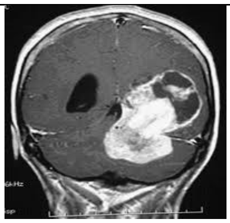
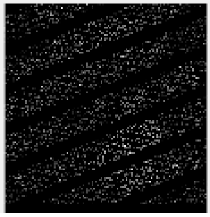
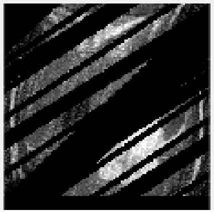
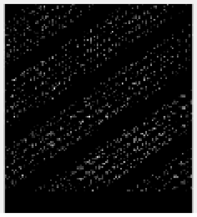
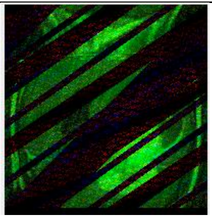
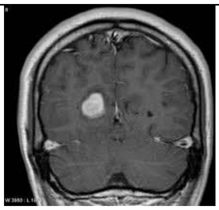
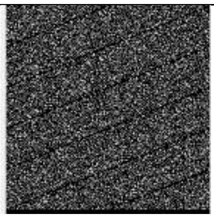
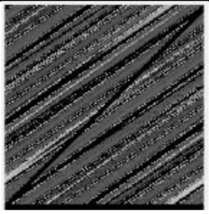
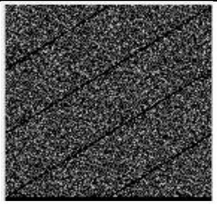
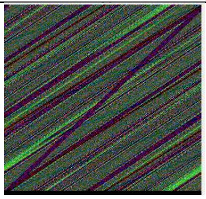
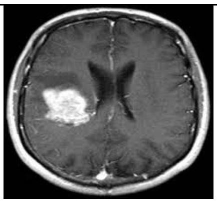
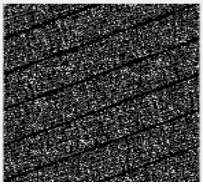
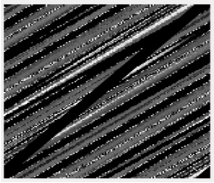
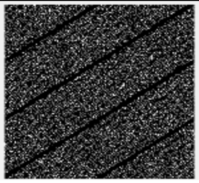
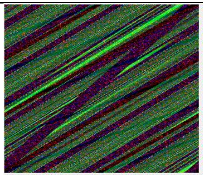
S.No	Original Input Image	Arnold iteration level 24	Arnold iteration level 48	Arnold iteration level 96	Arnold iteration level 200
1					
2					
3					
4					
5					

Table 2. Comparison of Steganography, Single LSB substitution and proposed method

Features	**Steganography method**	**Single LSB substitution method**	**Proposed method**
Encryption	**High**	**Low**	**High**
Capacity	**High**	**Low**	**High**
Robustness	**Medium**	**Low**	**High**
Interceptiblity	**High**	**Low**	**High**

Conclusions

In spite of availability of a number of encryption methods, research is still going on to develop methods satisfying all the requirements of Medical Image Encryption and data security. It is not that an easy task to develop a method that satisfies all the requirements as the Features Single, simple Arnold Transform method. Proposed method provide a good value for Interceptibility, Capacity, Robustness and Encryption, these values are varied with different methods. Future works in this direction include development of some transform domain methods those will provide robustness along with Interceptibility, security and insertion into higher order bits to achieve further higher capacity and robustness. It is observed that the proposed method gives greater scrambling choices This results in more chaos and better medical image encryption by providing a larger key space. The proposed transformation is an automorphism and both one-to-one and onto. Further, it preserves the area as well, given that the pixels lie in the same pixel map, following the transformation.

References

[1] Adhipathi Reddy and B.N.Chatterji.:A new wavelet based logo-watermarking scheme, Pattern Recognition Letters, 26:1019--1027, May 2005.

[2] F. A. Petitcolas, R.Anderson, and M. Kuhn: Information hiding: A survey, Proceedings of the IEEE, July 1999, vol. 87, pp. 1062—1078

[3] Neil F. Johnson: Steganography: Seeing the Unseen, George Mason University, http://www.iitc.com/stegdoc/sec202.html

DOI : https://doi.org/10.56452/7-80101

[4] RC Gonzalez, RE Wood: Digital Image Processing, 2nd Ed, PHI, New Delhi, 2006.

[5] A. Piva, M. Barni, F. Bartolini, and V. Cappellini.: DCT- based watermark recovering without resorting to the uncorrupted original image, In Proc. IEEE Int.Conf. Image Processing (ICIP 1997), 1997, pp.520-523.

[6] http://en.wikipedia.org/wiki/Arnold%27s_cat_map

[7] Changjiang Zhang et al., "Digital Image watermarking with Double encryption by Arnold Transform and Logistic", Fourth International conference on Networked Computing & advanced information Management, pp. 329-334, 2008.

[8] Manoj Kumar Meena et al., "Image Steganography tool using Adaptive Encoding Approach to maximize Image hiding capacity", IJSCE, Vol.1, pp. 7-11, May 2011

[9] Minati Mishra et al.: Steganography: the art of Secret Messaging through Digital Images, Proceedings of National Conference on Computational Intelligence and its applications (NCCIA-2007), pp.104-113, July 20

[10] H. Liu and C. Jin, A Color Image Encryption Scheme based on Arnold Scrambling and Quantum Chaotic, International Journal of Network Security, Vol. 19, No. 3, pp. 347-357 (2017).

[11] D.C. Mishra, R.K. Sharma, R. Ranjan and M. Hanmandlu, Security of RGB Image Data by Affine Hill Cipher over SLn(Fq) and Mn(Fq) Domains with Arnold Transform, Optik, Vol. 126, No. 23, pp. 3812-3822 (2015).

[12] L. Sun, J. Xu, X. Zhang and Y. Tian, An Image Watermarking Scheme using Arnold Transform and Fuzzy Smooth Support Vector Machine, Mathematical Problems in Engineering, 14 pages (2015).

[13] M.R. Abuturab, Generalized Arnold Map-based Optical Multiple Color-image Encoding in Gyrator Transform Domain, Optics Communications, Vol. 343, pp. 157-171 (2015).

[14] Z. Liu, M. Gong, Y. Dou, F. Liu, M.A. Ahmad, J. Dai and S. Liu, Double Image Encryption by using Arnold Transform and Discrete Fractional Angular Transform, Optics and Lasers in Engineering, Vo. 50, No. 2, pp. 248-255 (2012)