ISSN: 0975-766X
CODEN: IJPTFI
Available Online through
Research Article
www.ijptonline.com

A NOVEL CHAOTIC IMAGE ENCRYPTION SYSTEM FOR COLOR IMAGES BASED ARNOLD CAT MAP AND EFFICIENT PIXEL SHUFFLING

[1]Srinivas Koppu*, [2]Madhu Viswanatham
[1]School of Information Technology and Engineering, VIT University, Vellore, Tamil Nadu, India.
[2]School of Computing Science and Engineering, VIT University, Vellore, Tamil Nadu, India.
[1]School of Information Technology and Engineering, VIT University, Vellore, Tamil Nadu, India.
Email: srinukoppu@vit.ac.in

Received on 13-05-2016 *Accepted on 12-06-2016*

Abstract:

Image encryption is one of the most essential and crucial part in the process to prevent various security attacks. Chaotic methods are widely used in the latest encryption system for their variegated property. Encryption process is carried out by using Arnold cat map and chaotic shuffling process using magic matrix. The color component are decomposed individually with the help of Arnold cat map to perform the scrambling process this process is said to be permutation stage, then the shuffled elements are integrated by using pseudo-random keys. In this project we introduce a new Chaotic shuffling procedure using magic matrix to increase the randomness and complexity, which is efficient from existing methods and also makes encryption is much faster than others. Here encryption is done for color images and as well as medical images. The outcome of this encryption process will result in Image cipher. The decryption is done in the inverse method with the use of the key. Security tests and various performance analysis like Histogram analysis, NPCR and UACI analysis, key space analysis, PSNR analysis are carried out to prove that the proposed algorithm is efficient.

Keywords: Chaos, Arnold Cat Map, Image Cipher, magic matrix.

I. Introduction

Chaotic systems**:** Edward Lorenz is the first person to use chaotic theory in 1963. Chaos theory states-"When the present determines the future, but the approximate present does not approximately determine the future." Chaos based cryptography are very popularized in the past few years as it is well known for its high security by creating confusion by mixing up the pixels of the image. It has been broadly utilized as a part of picture encryption as it is exceptionally delicate to starting conditions, non-intermittent and very secure for correspondence which makes it unpredictable. Chaos theory is

one in which is highly adhesive towards the properties described by Shanon that are said to be perplexity and dispersion. Chaotic hypothesis got its begin in the field of ergodic hypothesis. Later concentrates, additionally on the theme of nonlinear differential mathematical statements were completed by George David Birkhoff, Mary Lucy Cartwright and John Edensor Littlewood and Stephen Smale. With the exception of Smale, these studies were all specifically motivated by material science: the three-body issue on account of Birkhoff, turbulence and galactic issues on account of Kolmogorov, and radio building on account of Cartwright and Littlewood. An early advocate of bedlam hypothesis was Henri Poincare. Chaotic systems are dynamic systems which are highly unpredictable after certain iterations; they are highly sensitive towards the initial conditions as a result any deviation in the initial conditions will lead to different results. Chaotic systems are well known for its randomness and sensitivity towards initial conditions which makes them very difficult to predict. Chaotic systems are widely utilized in the field of image encryption from past decade as they are non-periodic and highly secure for communication. Chaotic algorithms are of two types single chaotic system and multiple chaotic system. In multiple chaotic system, multiple single chaotic systems are merged to make it very complex and generate highly unpredictable sequence which in-turn improves the level of security. The complexity of the multiple chaotic algorithms are increased by using external keys. Chaotic systems are dynamic systems which are highly unpredictable after certain iterations, they are highly sensitive towards the initial conditions. Any slight changes in the initial parameters will result in multivariate results that are different from the previous or recorded results. As a result chaotic methods are very difficult to predict. Chaotic systems are almost similar to cryptographic algorithms that both are sensitive towards the initial conditions, unstable periodic orbits and random behavior. The well known basic principle of chaotic algorithms is that it uses random sequences which are used in the encryption procedure. Chaotic algorithms stand out due to this pseudo random behavior.

Arnold Cat Map: The first process is to rearrange the three color segments independently by utilizing Arnold Cat Map to reduce the relationship among neighboring pixels, the second process is carried out by integrating the shuffled color components with the random keys. The rearranging or the shuffling process is carried out by Arnold cat map due to its multiphase. This particular map is nothing but product of matrix N×N onto itself. This is shown as

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \begin{bmatrix} 1 & p \\ q & pq+1 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix} \bmod N \quad \text{- (1)}$$

The reverse procedure to de-shuffle the process is given by eqn(2),

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \begin{bmatrix} pq+1 & -p \\ -q & 1 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix} \bmod N \quad - (2)$$

Arnold cat map is well known for its complex randomization of the image pixels which ensures de-shuffling of the image after a particular number of iterations. Due to this property it is been widely used in different encryption algorithms. Randomization is not the only reason why lot of encryption methods use Arnold cat map it is because the decryption time of this system is comparatively faster and more efficient than other systems.. This system describes the flow of the phase space as bead hopping from one place to another whose position lies between an previously assumed standard conditions. All these features prove Arnold cat map chaotic behavior.

II. Materials and methods

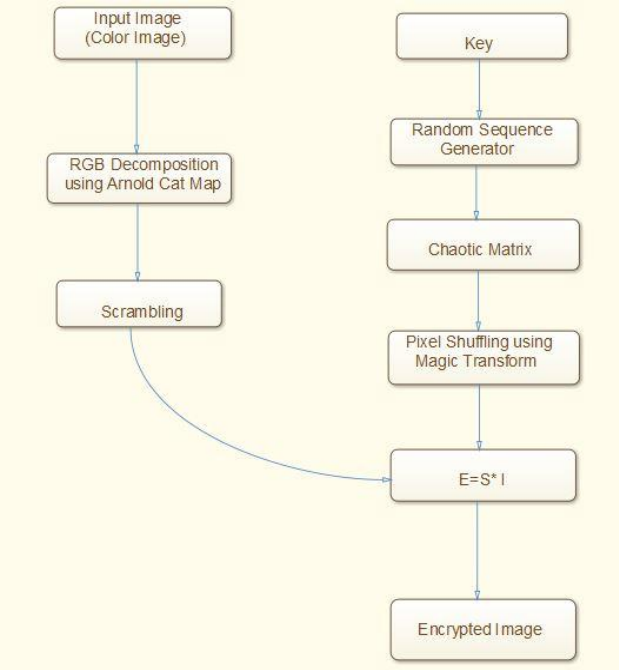


Fig. Architecture of the proposed system.

1. Architectural diagram

- A color image or an medical image can be provided as an input to the following system. Input image can be any image with variable length of pixels are accepted.
- Input color image or medical images are processed by using Arnold Cat map and decomposed into its corresponding R,G,B components where each colour components are processed separately and scrambling process takes place. The scrambling process shuffles or rearranges the pixels of each colour component so that the scrambled image is not similar to that of the original image. The resultant image S will be produced

- Key is generated using the chaotic magic matrix ,which is produced by using random sequence generator later the outcome of this process is used as the index matrix for Pixel shuffling process. The resultant image I will be produced at the end of this process.
- Encryption of the image is done by using S and I. The resultant of this process is encrypted image or cipher image.

Algorithm Module 1

1. Read the input image and decompose into respective colour matrix.
2. Using Arnold cat map the R,G,B components are scrambled by using predefined order which is produced using a random sequence generator.
3. The individual components are concatenated to form an scrambled image S

Algorithm module 2:

1. Consider a random matrix with size mxn where m represents the number of rows and m represents number of columns
2. The process of rearranging the pixels is done by using pixel shuffling method which is defined separately.
3. The scrambled image and shuffled image both are integrated to give cipher image or encrypted image.

2. Magic matrix

Definition: The numbering of the pixels is done in normal sequence order of integers as shown in fig.1. The entire matrix is considered to be collection of quadric matrix hence the shuffling is performed inside the quadric matrix that is 4 elements in the shape of infinity symbol in a clockwise direction which results in matrix M' as shown in fig.2. then Step 2 is repeated until it reaches the last cell. Result of this process is matrix M'' shown in fig.2 . Then the entire quad is considered as one cell and same shuffling process is carried out which results in matrix MS as shown in fig.4. Numbers in the shuffling process are colored to show the randomness of the shuffling order .

Step 1**:** Consider matrix M as the input matrix or the initial matrix. For(1,3,9,11) in M are connected with pixel in blue. For (2,4,10,12) in M are connected with pixel color yellow. For(6,8,14,16) in M are connected with pixel in green. For (5,7,13,15) in M are connected with pixel in pink

Step 2**:** (1,2,5,6) are shuffled in predefined order as shown in fig.2(M') which results in(5,6,2,1) $M_{1,1}=M_{0,0}(1)$, $M_{0,1=}M_{1,1}(6)$, $M_{1,0}=M_{0,1}(2)$, $M_{0,0}=M_{1,0}(5)$.

Step 3**:** Step 2 is repeated until it reaches the last quad , result of this step is as shown in fig.3(M'')

Step 4**:** Entire quad(5,6,2,1) is considered as single cell and the shuffling is performed which results in (13,14,10,9) and repeated for all four quads.

$M''_{(0,0),(0,1),(1,0),(1,1)} = M''_{(2,0),(2,1),(3,0),(3,1)}$ and as follows. Outcome of this step results in magic matrix MS.

Using this matrix MS the pixels of the original image are shuffled by replacing the corresponding pixels of the original image matrix IM.

3. Pixel shuffling:

Pixel shuffling is performed directly on the Original Image using a magic matrix whose size is same as that of the original image matrix. Magic matrix is generated by numbering the pixels using a normal sequence of numbers in the form of rows and columns but the shuffling order is determined by unique method which jumbles the pixels in maximum possible ways to remove the shuffling relation and make it more random and unpredictable as to increase the efficiency of the encryption . The shuffling process is carried out as follows

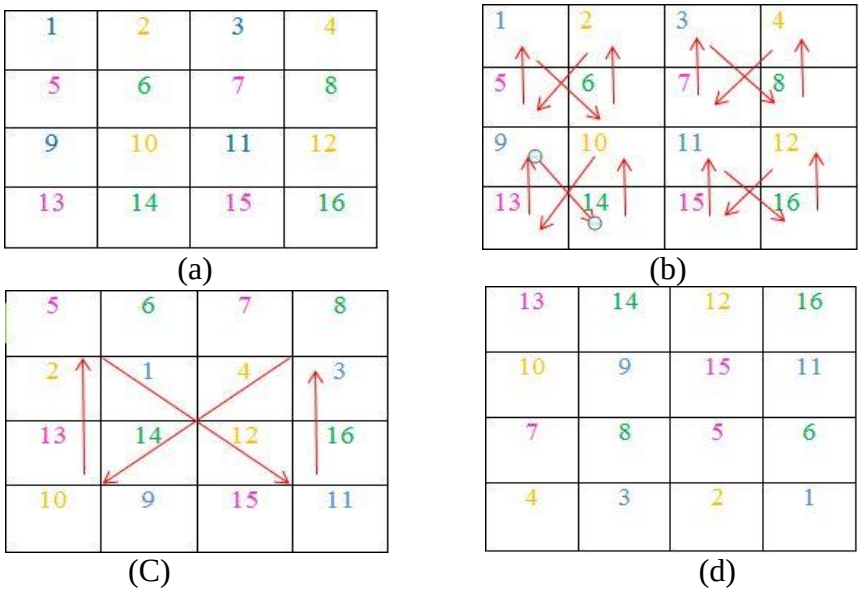


Fig2.Pixel shuffling

III. Results and discussion

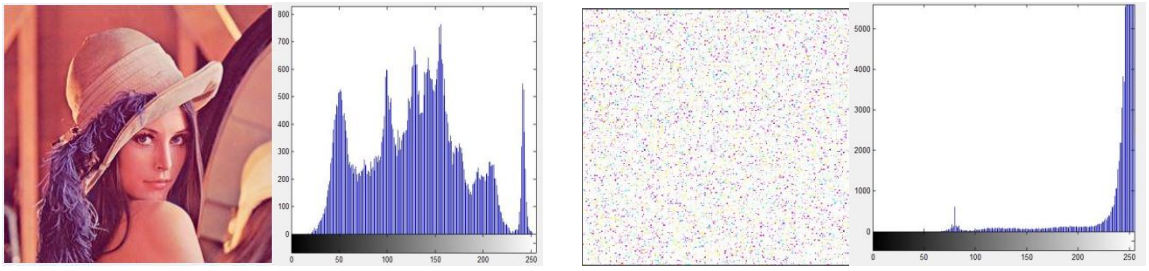
The experiment results shows the encryption process by using the the proposed system.It also shows encryption of various types of images and their corresponding analysis results.Encryption has been done and the following image is been processed and following encrypted image has been obtained image is produced. For example,,here lena image of size 256x256 is being encrypted and its corresponding output is shown

Original image **encrypted image**

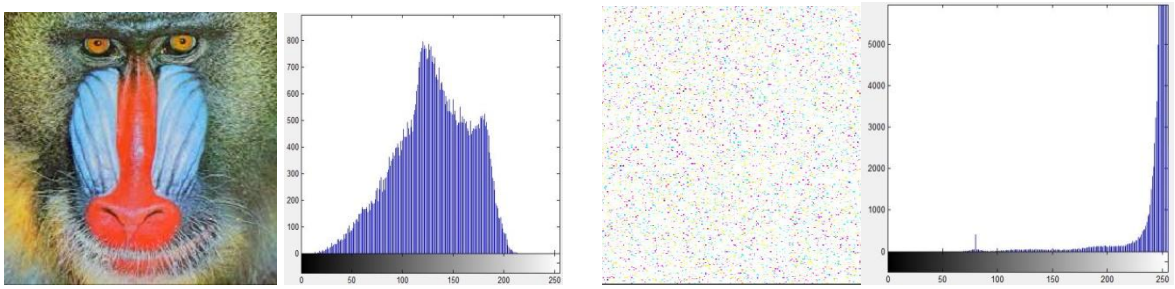
Fig.3 Lina image and its encryption.

1. Histogram analysis

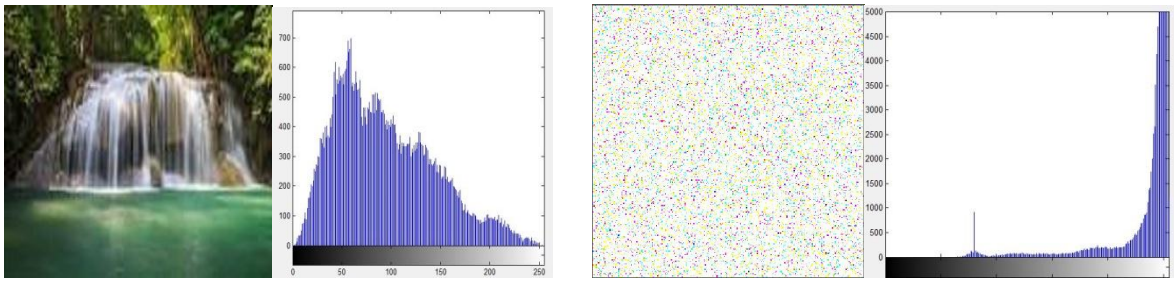
To analyze the encryption system three test images(lena, baboon and waterfall) are chosen and encryption is performed and corresponding histograms of original image and encrypted image are shown below. Here a,b,c are the original images and a',b' and c' are their respective histograms, then aa,bb,cc are encrypted images of a,b,c aand aa',bb',cc' are their corresponding histograms.



a a' aa aa'



b b' bb bb'



c c' cc cc'

Here we can clearly see that the histograms of original images and histogram of encrypted images are different and there are great changes in the pixel distribution of original and encrypted images.

2. Plaintext sensitivity analysis

The relation between the original image and the encrypted images are analyzed by the attackers to get the relation between them try to decrypt the image if the pixel distribution is similar and not random the encrypted is vulnerable to such kind of attacks, to measure these sensitivity we perform analysis like number of pixels change rate(NPCR) and unified average changing intensity (UACI).The NPCR measures the percentage of different pixel numbers between two images, whereas UACI measures the average intensity of differences between two images This analysis helps in determining the vulnerability of the system towards differential attacks. The analysis report for different images is given in the table.

Table1. NPCR and UACI analysis.

Input	NPCR	UACI
Baboon	98.23	24.14
Waterfall	99.98	32.93
Lena	99.89	47.76

3. Key security analysis

Key is produced by a random function generator so it is highly impossible to generate the same sequence of numbers and determine the key of each encryption used. The key space used in the system should be large enough to make the attack infeasible. The key space of the proposed system is said to be 2^8=256 and greater which is said to be large enough to avoid key space attacks and brute force attacks.

IV. Conclusion

Based on the results of the various analysis performed the novel chaotic algorithm is showed to be more efficient than the previous ones. Encryption and decryption is showed to be successful as the proposed framework can successfully encrypt and decrypt the input image. The key space of this algorithm is said to be 2^8=256 which is above normal and secure against the brute force attacks. The histogram analysis of various input images clearly shows that their corresponding chipered images have completely different histogram when compared to the original image which proves that the

algorithm is resistance against other differential attacks. Various survey analysis of npcr and uaci proves to be that Arnold cat map produces the efficient encryption when compared to other systems hence forth our system is proved to be efficient.

References

1. Kharat, P. H., & Shriramwar, S. S. (2015, May). A secured Transmission of data using 3D chaotic map encryption and data hiding technique. In Industrial Instrumentation and Control (ICIC), 2015 International Conference on (pp. 1243-1247). IEEE.
2. Zhe, Z., Haibing, Y., Yu, Z., Wenjie, P., & Yunpeng, Z. (2009, December). A block encryption scheme based on 3D chaotic Arnold maps. In Intelligent Interaction and Affective Computing, 2009. ASIA'09. International Asia Symposium on (pp. 15-20). IEEE.
3. Huang, J., & Long, M. (2009, September). A novel image cryptosystem with multiple chaotic maps. In Wireless Communications, Networking and Mobile Computing, 2009. WiCom'09. 5th International Conference on (pp. 1-4). IEEE.
4. Li, J., Xing, Y., Qu, C., & Zhang, J. (2015, September). An image encryption method based on tent and Lorenz chaotic systems. In Software Engineering and Service Science (ICSESS), 2015 6th IEEE International Conference on(pp. 582-586). IEEE.
5. Wu, X., & Wang, Z. (2015, January). A new DWT-based lossless chaotic encryption scheme for color images. In Computer and Computational Sciences (ICCCS), 2015 International Conference on (pp. 211-216). IEEE.
6. Fu, C., Tang, J., Zhou, W., Liu, W., & Wang, D. (2013, November). A symmetric color image encryption scheme based on chaotic maps. In Communication Technology (ICCT), 2013 15th IEEE International Conference on (pp. 712-716). IEEE.
7. Abdlrudha, H. H., & Nasir, Q. (2011, December). Low complexity high security image encryption based on nested pwlcm chaotic map. In Internet Technology and Secured Transactions (ICITST), 2011 International Conference for (pp. 220-225). IEEE.
8. Shang, F., Sun, K., & Cai, Y. (2008, May). An efficient MPEG video encryption scheme based on chaotic cipher. In Image and Signal Processing, 2008. CISP'08. Congress on (Vol. 3, pp. 12-16). IEEE.

9. Cheng, Y., Yang, S., & Li, S. F. (2010, September). Image Encryption of Multiple Keys Method Based on Chaotic Maps. In Pervasive Computing Signal Processing and Applications (PCSPA), 2010 First International Conference on (pp. 891-894). IEEE.
10. Qi-nan, L. I. A. O. (2011, May). TD-RECS Chaotic System Based Digital Image Encryption Algorithm Protecting from Shearing Attack. In Network Computing and Information Security (NCIS), 2011 International Conference on (Vol. 1, pp. 402-405). IEEE.
11. Chapaneri, S., Chapaneri, R., & Sarode, T. (2014, April). Evaluation of Chaotic Map Lattice systems for image encryption. In Circuits, Systems, Communication and Information Technology Applications (CSCITA), 2014 International Conference on (pp. 59-64). IEEE.
12. Fu, C., Lin, Y., Jiang, H. Y., & Ma, H. F. (2015, March). Medical image protection using hyperchaos-based encryption. In Medical Information and Communication Technology (ISMICT), 2015 9th International Symposium on(pp. 103-107). IEEE
13. Paral, P., Dasgupta, T., & Bhattacharya, S. (2014, April). Colour image encryption based on cross-coupled chaotic map and fractional order chaotic systems. In Communications and Signal Processing (ICCSP), 2014 International Conference on (pp. 1947-1952). IEEE.
14. Naveenkumar, S. K., & Panduranga, H. T. (2015, March). Chaos and Hill Cipher Based Image Encryption for Mammography Images. In Innovations in Information, Embedded and Communication Systems (ICIIECS), 2015 International Conference on (pp. 1-5). IEEE.
15. Ranjith, K. R., & Saranraj, B. (2014, November). A novel chaotic color image encryption/decryption based on triangular confusion. In Electronics, Communication and Computational Engineering (ICECCE), 2014 International Conference on (pp. 94-100). IEEE.
16. Sankpal, P. R., & Vijaya, P. A. (2014, January). Image Encryption Using Chaotic Maps: A Survey. In Signal and Image Processing (ICSIP), 2014 Fifth International Conference on (pp. 102-107). IEEE.

Corresponding Author:

Srinivas Koppu*,

Email: *srinukoppu@vit.ac.in*