Indian Journal of Science and Technology, *Vol 8(16), DOI: 10.17485/ijst/2015/v8i16/63545, July 2015*
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

An Efficient Three Layer Image Security Scheme using 3D Arnold Cat Map and Sudoku Matrix

P. Meenakshi* **and D. Manivannan**

School of Computing, SASTRA University, Thanjavur - 613401, Tamil Nadu, India; meena.esh@gmail.com, dmv@cse.sastra.edu

Abstract

In this paper, a three layer image cryptosystem for grayscale images is introduced to provide an efficient security for symmetric images. The proposed image encryption algorithm contains a 3D Arnold cap map for pixels' value shuffling and pixels' value substitution in the first layer. Followed by a Sudoku permutation layer which takes a Sudoku matrix and key as an input. The alternative block rotation mechanism is used to rotate the pixel values in the last layer. The confusion and diffusion properties of the 3D Arnold cat map together with Sudoku matrix and rotation provide good permutation and substitution for the image at each round. This proposed algorithm has a huge key space and has the desired secure cipher property. The security analysis is done in MATLAB, the simulation results demonstrates the robustness against differential attack models. The results conclude that the algorithm is best suitable for image encryption which requires efficient and fast encryption scheme.

Keywords: Chaotic 3D Arnold Cat Map, Image Encryption, Permutation, Substitution, Sudoku Matrix

1. Introduction

In the real world the transmission of confidential digital image over the network is growing in great need. In many cases such information leakage seriously invades unaccountable loss to the user. The importance of image security has been noticed and emphasized for recent years. This makes the researches to develop algorithms that mainly focus on providing security, accuracy and authentication of data resources. The various techniques for image encryption algorithm can be grouped into three major classifications: 1. Position permutation algorithms, permutates pixel positions of the image. 2. Value transformation algorithms, used to modify the pixel values of the image. 3. Visual transformation algorithm, changes the shape and size of the images.

In this work the main focus is to provide image security by using the 3D Arnold cat map for position based permutation. Normally the cat map return to the original pixel position after a certain number of iterations. Hence, to provide an additional level of encryption a Sudoku matrix is used for value based transformation and a rotation technique to scramble the pixel values.

The strength of any image encryption algorithm depends on the key space for encryption of the algorithm. In this for choosing a cat map nine parameters are used and for second level an NxN Sudoku matrix to generate. This increases the complexity of the encryption algorithm and also provides security to the image from many statistical attacks.

2. Related Works

Generalized 2D Cat map to 3D is used for designing a many secure symmetric chaotic image encryption algorithm; in this mostly a 3D cat map performs permutation of the position of image pixels in the permutation stage and employed a logistic chaotic system to diffuse the permuted image in the diffusion stage.

Thamizhchelvy et al.[1] design a new method for hiding the data using fractal image generation. The chaotic behavior of the fractal image, make it difficult to crack the system.

*Author for correspondence

Abninivesh[2], analyzed on secure data transaction on web service that generate keys dynamically alone the encryption and decryption process for distributed service system.

An Ant colony optimization method is used for optimizing the key generation process is proposed by Swapna et al.[3]. A combined technique of hashing algorithm is proposed by Ganeshkumar et al.[4]. This creates an identical digital fingerprint together with a key. Vidhya et al.[5], proposed an algorithm for steganography using ken ken puzzle.

Lian et al.[6], the authors firstly analyzed the sensitivity of the parameters for a standard chaotic map, and compared secret key space of standard map with that of cat map and baker map. The improved chaotic map was used for position permutation and a logistic map was used for image diffusion. Wang et al.[7] used logistic map for encrypting the color image which is cracked by Li et al.[8] Zhu et al.[9] proposed an algorithm by applying hyper chaotic sequences for key steam generation, which is proved as it is not withstand for chosen plain text attack. Wang et al.[10] designed a cryptosystem using perception model combined with Lorenz map, but Zhang et al.[11] cracked the algorithm. The disadvantage of Wang's algorithm is changing a single bit in the original image will change only one bit in encrypted image.

A general Architecture for cryptosystem based on a chaotic map was designed by Alvarez and Li[12] and also discussed on the important issue on implementation, key management and security analysis. Later, Alvarez et al.[9] analyzed the practical security using the Baker map in strictly adhering to the basic guidelines for security in acceptable level.

Guan et al.[13] combined the Arnold cat map and Chen map. ACM is used for scrambling the pixel data, then XOR with Chen map output. Xiao et al.[14] improved this algorithm. A Novel two stage algorithm with ACM and sequence sorting was proposed by Fu et al.[15] Which has minimum computational overhead and more secure. Fouda et al.[16] designed fast and secured block cipher cryptosystem to solve the drawback in the time-consuming arithmetic calculation of real numbers.

Chen et al.[17] used 3D or higher dimensional maps for diffusion and confusion by swapping of pixel values. This efficient scheme overcomes the weakness of the chosen / known plaintext attacks. Moreover, in every round a single change in pixel value makes a huge difference in the outcome. Yue Wu et al.[18] designed a scheme using Latin square and a new 2D matrix for substitution–permutation for a good confusion and diffusion maintenance with more tolerance for error.

In this work a three layer encryption algorithm for binary images based on improving chaotic 3D Arnold cat maps[19] and Sudoku matrix. The 3D chaotic maps with randomly selected initial conditions are highly sensitivity is used for first level of encryption and a NxN, Sudoku matrix is used for the next level of security and in the last level, a block based rotation is used. The proposed paper is organized as following sections. In the next section, a short note on Sudoku matrix, followed by an introduction to chaotic 3D cat map. The proposed algorithm is discussed in Section 4. Simulation results and security analysis are described in section 5. Finally section 6 concludes the paper.

3. Arnold Cat Map

The traditional methods like DES, AES are not suitable for image application due to relatively small block size, the nature of digital image, bulky data capacity and high correlation among the pixels. To solve this high computational workload of conventional algorithm, Fridrich et al.[15] proposed a 2D discrete chaotic baker map for an image encryption system. This confusion and diffusion form the basic structure for most of the chaos based image encryption methods. Due to their property of ergodicity, aperiodicity, sensitivity to initial conditions and sensitivity to control parameters, etc., makes chaotic maps have a good potential for information encryption, especially image encryption. Image encryption algorithms based on 1D or multi dimensional chaotic maps have been proposed digital image encryption algorithm[16].

Chaotic maps are quickly iterative simple functions which much enough for real-time applications. In chaotic map a ten-millionth change in the initial parameters makes a huge effect on the output. Chaotic maps are of two types; continuous and discrete.

Many researchers noted that highly sensitive nature of the initial condition, with the confusion and diffusion behavior make chaotic map aids for designing complex image security algorithms. The discrete chaotic maps are more suitable for image security. Every map has some parameter which forms the encryption key. Depending on the image security scheme (stream or block), type of map and its initial condition must be selected.

Arnold Cat Map (ACM) or Arnold transforms is a type of discrete system which shears and folds the images mathematically into itself in phase space, which is a typical

character of chaotic map. This confusion and diffusion property of the ACM makes it more suitable for image security. The General notation for 2D cat map used for image encryption can be given by eq. (1), which has two control parameter, P and Q. A digital image can be seen as 2D matrix in which (x, y) represents the pixel position in the image. After performing the 2D Arnold scrambling it becomes x' and y', the new pixel position as in eq (2). This makes the traverse of the pixel movement completely within the size of the image (M).

$$A = \begin{pmatrix} 1 & P \\ Q & PQ+1 \end{pmatrix} \tag{1}$$

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = A \begin{bmatrix} x \\ y \end{bmatrix} mod\ M \tag{2}$$

The invertible matrix for the decryption process exists when its determinant is 1 and its largest Lyapunov exponent must be strictly positive, given by ln σ1.

The number of the rounds in the Arnold cat map is not directly proportional to the size of the image but related[15]. Generally a 2D cat map can be extended to a 3D chaotic map were used for image encryption by introducing six parameters. In this work a improved 3D Arnold cat matrix in eq (3) is used for image encryption[14]. The benefit of choosing this improved 3D cat map is the more number of parameters involved in forming the matrix. This increases the complexity of the decryption and also makes the algorithm to withstand from many statistical attacks. The new parametric 3D map has 8 independent parameter, 2 controlling spatial configurations and 6 controlling matrix elements. Thus the new 3D cat map family have more parameters but correlated matrix compared to present 3D map[17]. Consider a 3D Cat Map (CM) of eq(3), where , elements a = 1, e = bd+1 = ab+1, i = cg+fh-bfg-cdh+bcdg+1 = cd+(bc)(abcd)-abcd-cb(abcd)+acbd+1.

$$CM = \begin{pmatrix} a & b & c \\ d & bd+fh-bfg-cdh+bcdg+1 & f \\ g & h & cg+1 \end{pmatrix} \tag{3}$$

4. Description of Proposed Algorithm

The Reasons for choosing a 3D cat map is it provides more security than other chaotic maps. The 3D cat map is simpler to implement and it is more suitable for symmetric image encryption. Each round in the proposed algorithm contains mainly three modules as shown in Figure 1.

4.1 3D ACM Cipher

The main purpose of a 3D cat map is used for scrambling the pixel position along with the modified pixel value. This makes each and every pixel values are placed in a new location with new value. In this a 3D cat map is used over a module of M as a finite system as in eq (4), where the vector [x', y', z'] is the scrambled position of the vector [x,y,z], where x, y is the coordinate position of the pixel value z. Pixels are placed in the position according to the following process

$$\begin{bmatrix} x' \\ y' \\ z' \end{bmatrix} = CM * \begin{bmatrix} x \\ y \\ z \end{bmatrix} mod\ M \tag{4}$$

The coordinates (x, y) of the pixel and the control parameter of the coupled map as the initial conditions, map is iterated. Then the position of pixels from the image to scrambled image can be obtained. The pixels will get different chaotic positions, so the pixels will spread in a random manner.

4.2 Sudoku Permutation

4.2.1 Key Generation

The Key generation process has two input, A Key (Key_1) and a Sudoku Matrix (SM) to produces the permutation sequences (P_Seq) of N^2 elements with values ranges

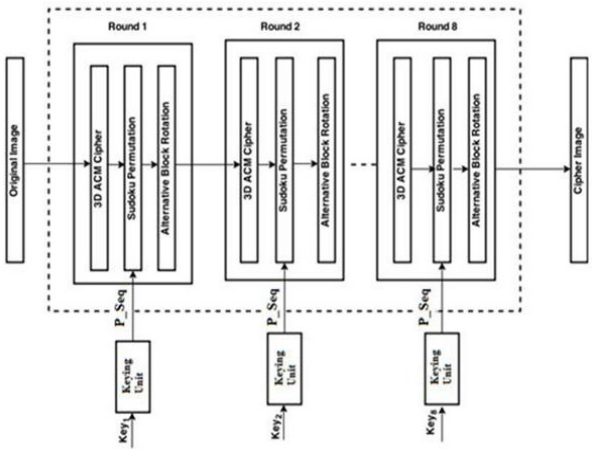

Figure 1. Block diagram of Encryption process.

from 0-255. The Key_1 in eq(6)consist of N numbers and it is formed as per the eq(5) .

$$K_i = \{x \mid x \in [0,N)\} \quad (5)$$

$$Key_1 = K_0, K_1, ..., K_{N-1}, K_i \neq K_j \text{ where } i,j = \{0,1,\ldots.N-1\} \quad (6)$$

Every element in the SM can be specified by block number (b_i), in the particular block by row (r_i) and column (c_i) value. In the new block (b_i), the row and column can be given by r_i and c_i. Rearrange the blocks of SM according the value of the Key_1. This makes the complete movements of all the blocks of SM. Now this New SM Matrix is the P_Seq which is NxN matrix. Specifically the Key generation process is done by Algorithm 1.

Algorithm 1: Key Generation Process
Input: SM (Sudoku Matrix NxN), Key_i
Output: P_Seq (NxN Matrix)

1. for i = 0 to N*N-1
   Newblock (b_i)=value(e_i)
   row (r_i) =oldblock(e_i) /4
   column (c_i) = oldblock(e_i)%4
   end for
2. for i= 0 to N/4 - 1
   for j=1 to N/4 -1
   $Key_1[i][j] = K_{i+j}$
   end for
   end for
3. for i= 0 to N-1
   SM ($block_i$)= $Key_{1(K_i)}$
   end for
4. for i=0 to N-1
   for j =0 to N-1
   New SM[i][j]=N * K_{i+j}+old SM[i][j];
   end for
   end for

4.2.2 Sudoku Permutation

The standard gray scale image (512x512) for image processing is taken. The image after subjected to 3D ACM cipher layer is given as into this layer .It is divided into four blocks of 256x256. In this conventional block cipher, the Sudoku Permutation normally scrambles or shuffling the pixel values with the P_Seq. The P_Seq can also be described as bijection. The steps to perform are specified in Algorithm 2. This makes the value change in the matrix along with position permutation. After performing the permutation the images is divided into block of NXN and each block is ex-or with SM matrix.

Algorithm 2: Sudoku Permutation

Input: Image (I),P_Seq
Output: Scrambled Image

1. Divide the Image into 4 parts of 256x256,each $I_i = \{0,1..4\text{-}1\}$
2. do
   {Each pixel value in the I_i is scrambled as,
   2.1. Value= $I_i[i][j]$
   2.2. R=P_Seq[i][j]/4
   2.3. C= P_Seq[i][j]%4
   2.4. $I_i[R][C]$=Value.
   }
3. Repeat for all the block

4.3 Alternative Block Rotation Phase

For a gray scale image I of size MxM, it is an integer matrix of M rows and M columns. Thus, a pixel value of the image I_{MxM} is rotated into a matrix of image of size I^*_{MxM}.

- Divide I into non-overlapping blocks based on value D, as in eq (7).

$$D = \frac{M-r}{n}, \text{where } r = 0 \quad (7)$$

- Assume 16 can divide M, and there L (M/16)blocks of 16x16 , B(1),B(2),…,B(L). The pixel value for each block is based on the position pointed at Figure 2 and Figure 3 demonstrates the rotation process of each block.
- Firstly the horizontal rotation is done as shown in the Figure 2, followed by the vertical rotation as in Figure 3. The Algorithm 3 describes the steps to perform the alternative block rotation.

Figure 2. Alternative Block Rotation. **(a)** Vertical Rotation Phase, **(b)** A Sample 4x4 Image Block and **(c)** Result After Vertical Rotation Phase.

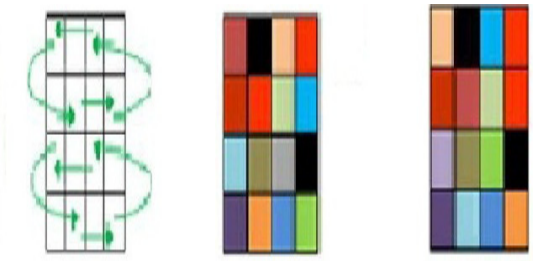

Figure 3. Alternative Block Rotation - Horizontal. **(a)** Horizontal Phase, **(b)** A Sample 4x4 Image Block and **(c)** After Horizontal Phase.

Algorithm 3: Alternative Block Rotation phase (I)

Input: Image I (MxM).
Output: Cipher Image, C (MxM).

```
d=(M-r)/n
while ( d>0)
for r =0 to N² -1
   for c=0 to N² -1
      blockrow=(r/128);
      blockcol=(c/128);
      outRow=128*(rotateOrder[blockrow]
         [blockcol]%4)+r%128;
      outCol=128*(rotateOrder[blockrow]
         [blockcol]/4)+c%128;
      I[i][j]=I[i][j]+(i*512)+c )%256
     decrement d;
repeat for all other blocks.
```

5. Performance Analysis

5.1 Key Space Analysis

The encryption algorithm should be large to provide high security and to withstand the brute force and statistical attack. In this proposed paper on chaotic image encryption algorithm, if image size is 512 and the Sudoku matrix is of 16x16 then the key space consists of (1) 3D Arnold cat map parameters (a, b, c, d, e, f, g, h, i) with the complexity of (2^9) , (2) NxN Sudoku matrix which is converted as P_Seq. (3) Key_1 a random sequence of 16 numbers which has the complexity of 16^{16} .Then the key space for the algorithm is very huge with additional complexity of determining the Sudoku matrix. The same amount complexity is applicable for the reverse process.

5.2 Differential Analysis

The need for differential analysis is an attacker can modify some pixel values in the original image and traces the difference in the cipher image in order to know the meaningful relation between them. This is chosen/known plaintext attack. A Secure cipher image must be sensitive even to a small modification. The NPCR & UACI are quantitative and qualitative scores for the strength against possible differential attacks of image ciphers. For a secure NPCR score must be larger and UACI score must not be larger. Table 1 show the NPCR and UACI values for various images. The histogram of the encrypted image is distributed nearly a uniform manner and differs from the original image histogram. This shows statistical attack entirely infeasible. The proposed image encryption algorithm is analyzed over the various standard image encryptions which is described in the Figure 4, Figure 5 and Figure 6.

Table 1. NPCR and UACI values for various images

Image name	NPCR value	UACI value
Lena.png	0.9654	0.2621
Barbara.png	0.9348	0.2976
Baboon.png	0.9561	0.2823

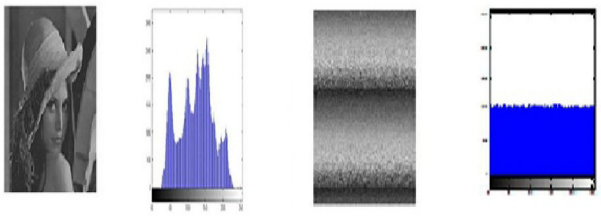

Figure 4. Analysis for Lena Image. **(a)** Original Lena image, **(b)** Histogram for original image, **(c)** Encrypted of original image of Lena and **(d)** Histogram for Encrypted image.

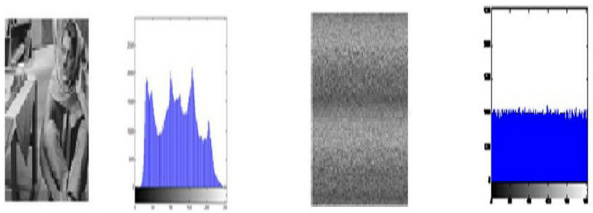

Figure 5. Analysis for Barbara Image. **(a)** Original Barbara Image, **(b)** Histogram for Barbara Image, **(c)** Encrypted of Original Image of Barbara and **(d)** Histogram for Encrypted Image.

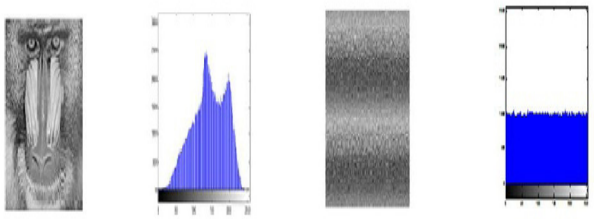

Figure 6. Analysis for Baboon Image. **(a)** Original Image of Baboon, **(b)** Histogram for Baboon Image, **(c)** Encrypted of Original Image of Baboon and **(d)** Histogram for Baboon Image.

6. Conclusion

In this paper, a three layer cryptosystem is proposed for encrypting the image. The 3D Arnold cat map and the Sudoku matrix are used. Improving the security by increasing the randomness in the image and larger key space in every stage is the advantages of this scheme, 3D ACM with different parameter at each round reduce the undesirable outcome. Sudoku matrix generated is unpredictable due to the number of combinations of the matrix which adds the security to matrix. The results for standard images has been demonstrated which shows the resistance of the cipher image to chosen/known plaintext attack. As the future work, other gaming techniques can be incorporated to generate the key sequence and initial condition.

7. References

1. Thamizhchelvy K, Geetha G. Data hiding technique with fractal image generation method using chaos theory and watermarking. Indian Journal of Science and Technology. 2014; 7(9):1271–8.
2. Abhinivesh M, Garg M, Acharjya D. Secured transaction for distributed service system. Indian Journal of Science and Technology. 2015; 8(S2):160–4.
3. Sasi SB, Sivanandam N. A survey on cryptography using optimization algorithms in WSNs. Indian Journal of Science and Technology. 2015; 8(3):216–21.
4. Ganeshkumar K, Arivazhagan D. Generating a digital signature based on new cryptographic scheme for user authentication and security. Indian Journal of Science and Technology. 2014; 7(S6):1–5.
5. Vidya G, Preetha RH, Shilpa G, Kalpana V. Image steganography using ken ken puzzle for secure data hiding. Indian Journal of Science and Technology. 2014; 7(9):1403–13.
6. Lian S, Sun J, Wang Z. A block cipher based on a suitable use of the chaotic standard map. Chaos, Solitons & Fractals. 2005; 26(1):117–29.
7. Wang X, Teng L, Qin X. A novel colour image encryption algorithm based on chaos. Signal Processing. 2012; 92(4):1101–8.
8. Li C, Zhang LY, Ou R, Wong K-W, Shu S. Breaking a novel colour image encryption algorithm based on chaos. Nonlinear dynamics. 2012; 70(4):2383–8.
9. Alvarez G, Li S. Breaking an encryption scheme based on chaotic baker map. Physics Letters A. 2006; 352(1):78–82.
10. Wang X-Y, Yang L, Liu R, Kadir A. A chaotic image encryption algorithm based on perceptron model. Nonlinear Dynamics. 2010; 62(3):615–21.
11. Zhang Y, Li C, Li Q, Zhang D, Shu S. Breaking a chaotic image encryption algorithm based on perceptron model. Nonlinear Dynamics. 2012; 69(3):1091–6.
12. Alvarez G, Li S. Some basic cryptographic requirements for chaos-based cryptosystems. International Journal of Bifurcation and Chaos. 2006; 16(08):2129–51.
13. Guan Z-H, Huang F, Guan W. Chaos-based image encryption algorithm. Physics Letters A. 2005; 346(1):153–7.
14. Xiao D, Liao X, Wei P. Analysis and improvement of a chaos-based image encryption algorithm. Chaos, Solitons & Fractals. 2009; 40(5):2191–9.
15. Fu C, Lin B-B, Miao Y-S, Liu X, Chen J-J. A novel chaos-based bit-level permutation scheme for digital image encryption. Opt Commun. 2011; 284(23):5415–23.
16. Fouda JAE, Effa JY, Sabat SL, Ali M. A fast chaotic block cipher for image encryption. Communications in Nonlinear Science and Numerical Simulation. 2014; 19(3):578–88.
17. Chen J-X, Zhu Z-I, Fu C, Yu H, Zhang L-B. A fast chaos-based image encryption scheme with a dynamic state variables selection mechanism. Communications in Nonlinear Science and Numerical Simulation. 2015; 20(3):846–60.
18. Wu Y, Zhou Y, Noonan JP, Agaian S. Design of image cipher using latin squares. Information Sciences. 2014; 264:317–39.
19. Wu Y, Agaian S, Noonan JP. A new family of generalized 3D cat maps. ArXiv preprint. ArXiv: 12053208. 2012.
20. Li M, Liang T, He Y-J, editors. Arnold transform based image scrambling method. 3rd International Conference on Multimedia Technology; 2013.
21. Liu H, Zhu Z, Jiang H, Wang B, editors. A novel image encryption algorithm based on improved 3D chaotic cat map. The 9th International Conference for Young Computer Scientists (ICYCS 2008); 2008; IEEE.
22. Lian S, Mao Y, Wang Z, editors. 3D extensions of some 2D chaotic maps and their usage in data encryption. Proceedings 4th International Conference on Control and Automation (ICCA'03); 2003; IEEE.