International Journal of
Intelligent Systems and Applications in Engineering

ISSN:2147-6799 www.ijisae.org Original Research Paper

An Efficient Image Encryption Algorithm for the Period of Arnold's CAT Map

Deniz ELMACI[1], Nursin BAS CATAK[*2]

Accepted : 05/03/2018 Published: 30/03/2018

Abstract: Arnold's CAT Map (ACM) is a chaotic transformation of the 2-dimensional toral automorphism T^2 defined by the mapping $\Gamma : T^2 \to T^2$. There are many applications of ACM in various research areas such as: steganography, encryption of images, texts and watermarks. The transformation of an image is achieved by the randomized order of pixels. After a finite number of repetitions of the transformation, the original image reappears. In this study, encryption of two images is demonstrated together with a proposed algorithm. Moreover, the periodicity of ACM is discussed and an algorithm to change the period of ACM is suggested. The resultant period obtained from the new algorithm is compared with the period obtained from the usual ACM. The results show that the period of the proposed algorithm grows exponentially while the period of ACM has an upper bound.

Keywords: *Arnold's CAT map, Chaos, Discrete-time dynamical systems, Hyperbolic toral automorphism.*

1. Introduction

ACM is a well-known example of Anosov diffeomorphism which is a map on a manifold M defined by a compact and smooth function f, from M to itself, $f : M \to M$. An Anosov diffeomorphism satisfies the following conditions: [1]

(a) There is a continuous splitting of the tangent bundle $TM = E^S \to E^u$ which is preserved by the derivative df.
(b) There exist constants $C > 0, C' > 0$ and $\lambda \epsilon (0,1)$ and a Riemannian metric $\|\ \|$ on TM such that $\|df^n(v)\| \leqq C\lambda^n\|v\|$.

Moreover, the Anosov diffeomorphism is a field of dynamical systems. A dynamical system is defined as a set of relationships among two or more measurable quantities and the evolution of the quantities over time is described by a fixed rule. A state vector $\mathbf{x} \in \mathbb{R}^n$, and a function $f : \mathbb{R}^n \to \mathbb{R}^n$ which describes how the system evolves over time, define the dynamical system. Additionally, dynamical systems can be considered in two types: a discrete time dynamical system and a continuous time dynamical system.
The discrete time dynamical system is specified by the following system of equations:

$$\mathbf{x}(0) = \mathbf{x}_0$$

$$\mathbf{x}(k+1) = f(\mathbf{x}(k)) \quad (1)$$

where k denotes the time.
And, the continuous time dynamical system is characterized by the following equations [2],

$$\mathbf{x}(0) = \mathbf{x}_0$$

$$\mathbf{x}' = f(\mathbf{x}) \quad (2)$$

[1,2] *Department of Mathematics, Ege University, Izmir– 35100, TURKEY*
** Corresponding Author: Email: nursin.catak@ege.edu.tr*

Systems of linear equations represent simple movements and their solutions are a space of analytic functions. However, the analytical solutions of many equations can be impossible. In order to obtain a function from the solution, initial or boundary conditions that determine the function are needed. If an analytical solution can be found, well-defined boundary conditions pick a single function from the solution space. This phenomenon has an analogous with the determinism which expresses the current status of a physical system depending on the result of its previous status. Besides, if an analytical solution space does not exist, then both the initial conditions with certain function cannot be chosen and initial conditions cannot be determined exactly. This situation creates a phenomenon that is called chaos [3].
The basic property of the Chaos Theory is that it is very sensitive to the initial conditions. That is, a small change in the initial condition results in a change, which cannot be predictable [4].
The main principles of the Chaos Theory can be stated as follows:

(i) Order creates disorder,
(ii) There is an order in disorder,
(iii) The system can't be said irregular if the order is not understood.

Hence, it is impossible to get out of the order.

1.1. Literature Review

A Russian mathematician Vladimir Igorevich Arnold described a continuous automorphism on the torus (CAT) in 1960's. He preferred to apply the CAT map to an image of a cat by analogizing of the capital letters of the Continuous Automorphisim of the Torus. A chaotic dynamical system can be built by using the CAT transformation. The transformation of an image is achieved by randomizing order of pixels. When iteration is repeated enough number of times, then the original image reappears [5]. Since the original image reappears after a several number of transformations, the periodicity of the CAT map aroused many researchers' interest. The first research on the period problem of the CAT map was done by Keating et al. They discussed an approximation solution for the

CAT map by combining the number theory and probability for the prime number data of N dimension. In their work, the exact solutions for the period distribution were not obtained. However, an approximated solution when N goes to infinity is obtained [6]. The problem of period is solved by Dyson and Falk. They determined an upper bound of the period is determined with the lack of partial and asymptotic results [7]. On the other hand, W.Chen et al. used an interference method to encrypt a color image based on CAT map [8]. Zhengjun Liu et al. designed a color image encryption algorithm by using Arnold transform and discrete cosine transforms [9]. Xiangjun Wu et al. proposed a new robust color image encryption scheme based on multiple improved 1D chaotic system and DNA sequence operations [10]. Ali Soleymani et al. used the Arnold CAT and Henon chaotic maps for securing images in order to create secret images and by using specific parameters for the permutation [11]. Recently, Zhi Li et al. used piecewise linear chaotic maps to encrypt a bit-level image [12]. N.K. Gursoy and U. Nuriyev are proved lower and upper bounds for some inequalities [13]. Furthermore, double random phase encoding and Arnold's CAT map is used for optical image encryption by A.Q. Alhamad [14]. Hua Chen et al. used a hyper-chaos-based image encryption algorithm [15]. L.Huang et al. proposed a difference of the output sequences of two same existing 1D chaotic maps[16].

2. Arnold's CAT Map

ACM is a simple demonstration of the Chaos Theory. The algorithm of the transformation is constructed by converting an image to an appropriate number of pixels for generating an $N \times N$ matrix. The coordinates of each pixels is stated by an ordered pair of (X, Y) in the real interval $[0, 1)$.

A special matrix of ACM for the transformation of all pixels is defined as follows:

$$A = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \tag{3}$$

Each coordinate in the interval $[0, 1)$ is normalized in order to avoid the dimension of resultant matrix to be increased after the transformation by taking in mod 1 [17].

Accordingly, the new position of any pixel is determined by using the transformation matrix as in the following equation:

$$\Gamma_{cat}\begin{pmatrix} x_{n+1} \\ y_{n+1} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}\begin{pmatrix} x_n \\ y_n \end{pmatrix} \ (mod\ 1) \tag{4}$$

where $\Gamma_{cat} : T^2 \to T^2$

and x_{n+1} , y_{n+1} are obtained as follows:

$$x_{n+1} = x_n + y_n$$

$$y_{n+1} = x_n + 2y_n \tag{5}$$

The mapping in the (4) known as the 2-dimensional toral automorphism T^2 is defined by $\mathbb{R}/\mathbb{Z} \times \mathbb{R}/\mathbb{Z}$. A diagram of a Torus is represented in the Fig. 1.

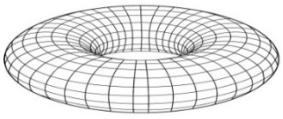


Fig. 1. A sketch of a Torus.

If the image has a rational coordinates i.e.; $0 \le \frac{x}{N}, \frac{y}{N} < 1$, then a scaling of the coordinates can be done to work with the integer coordinates $0 \le x, y \le N - 1$ [17]. Therefore, modulo N can be taken instead of modulo 1 for normalization.

Consequently, a general CAT map can be written by using the (4) following equations:

$$A = \begin{pmatrix} 1 & p \\ q & pq + 1 \end{pmatrix} \tag{6}$$

$$\Gamma_A\begin{pmatrix} x_{n+1} \\ y_{n+1} \end{pmatrix} = \begin{pmatrix} 1 & p \\ q & pq + 1 \end{pmatrix}\begin{pmatrix} x_n \\ y_n \end{pmatrix} \ (mod\ N) \tag{7}$$

where $\Gamma_A : Z_N \times Z_N \to Z_N \times Z_N$

The transition from the rational coordinates in the interval $[0, 1)$ to the integer coordinates $(0,1,2, \dots , N-1)$ is shown in Fig.2.

$$\begin{array}{ccc} T^2 & \xrightarrow{\Gamma_{cat}} & T^2 \\ \downarrow{\scriptstyle \pi} & & \downarrow{\scriptstyle \pi} \\ \mathbb{Z}_N \times \mathbb{Z}_N & \xrightarrow[\Gamma_A]{} & \mathbb{Z}_N \times \mathbb{Z}_N \end{array}$$

Fig. 2. A Transition of the Γ_{cat} and Γ_A

Where q is a position variable $0 < q < N$ and p is a momentum variable, with $p_t = q_t - q_{t-1}$, and N is the dimension of the image. In this study, values of p and q are taken to be 1 to simplify the relationship between CAT map and Fibonacci series.

The matrix A is a symmetric matrix and its eigenvectors are orthogonal. That's why, the discrete time dynamical system holds the Poincare Recurrence Theorem. Poincare Recurrence Theorem points out that certain systems return to a state very close to the initial state after a finite time interval. This gives an idea about the periodicity of the system.

2.1. The Linear Feedback Shift Register

The sequence given in (6) can be modeled as Linear Feedback Shift Register (LFSR) sequence. That can be analyzed using the generating function approach. The period distribution problem can be systematically investigated in the following three cases:

$(Z_n , + , \times)$

i. a Galois field,
ii. a Galois ring,
iii. a general commutative ring.

By taking the above three cases, it can be concluded that; N is a prime number, N is power of prime number or N is a composite number [18].

LFSR is a shift register whose input bit is a linear function of its previous state. LFSR sequence is a sequence $(a_i),\ i \in N$ satisfying the recursion

$$a_{i+n} = \sum_{j=0}^{n-1} c_j . a_{i+j} \tag{8}$$

3. The Linkage Between ACM and Fibonacci Series

The Fibonacci sequence is a series of numbers that is found by adding up two successive previous numbers. That is, 0, 1, 1, 2, 3, 5, 8, 13 .... Fibonacci numbers appear in many natural events such as; patterns of sunflowers, the bracts of pinecone, swirls of hurricanes and galaxies. For that reason, they are great interest of biologists and physicists. The Fibonacci sequence is usually denoted by F_n.

The following recurrence relation defines a Fibonacci sequence:

$$F_n = F_{n-1} + F_{n-2} \tag{9}$$

which is written in the matrix form as:

$$F = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} F_0 & F_1 \\ F_1 & F_2 \end{pmatrix} \tag{10}$$

The n^{th} power of the matrix in (10) is defined by:

$$F^n = \begin{pmatrix} F_{n-1} & F_n \\ F_n & F_{n+1} \end{pmatrix} \tag{11}$$

When the square of the matrix F is calculated, a special matrix of ACM is obtained:

$$F^2 = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} = A \tag{12}$$

By using the (11) the n^{th} iteration of A^n is written as [17]:

$$A^n = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}^n = F^{2n} = \begin{pmatrix} F_{2n-1} & F_{2n} \\ F_{2n} & F_{2n+1} \end{pmatrix} \tag{13}$$

4. The Periodicity of ACM

A period can be described as the completion of a cycle. A system is called periodic when it returns to its initial state after certain of time interval. In CAT map, if the transformation is repeated enough number of times, then it will return to the initial state. However, the period of the discrete CAT map does not always become greater with an increasing modulo. Since the period of a discrete CAT map doesn't always increase with increasing the parameters, it yields a necessity to discuss the relationship of the period with its modulo and with its parameters. Accordingly, by using the Γ function defined in (4), the following relation is obtained:

$$\Gamma\begin{pmatrix} x_{n+1} \\ y_{n+1} \end{pmatrix} = A^k \begin{pmatrix} x_n \\ y_n \end{pmatrix} \ (mod\ N) \tag{14}$$

where A^k has the form as:

$$A^k = \begin{pmatrix} F_{2k-1} & F_{2k} \\ F_{2k} & F_{2k+1} \end{pmatrix} \ (mod\ N) \tag{15}$$

and F_{2k-1} and F_{2k} should satisfy the following equality:

$$\begin{aligned} F_{2k-1} &\equiv 1\ (mod\ N) \\ F_{2k} &\equiv 0\ (mod\ N) \end{aligned} \tag{16}$$

The value of k is a period of CAT transformation, but it isn't necessary to be the minimal period. For that reason, Pisano period is examined whether the obtained period is the minimal period or not.

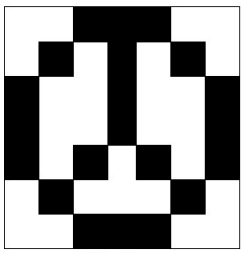
4.1. Pisano Periods

The Pisano period is the length of the sequence of Fibonacci numbers, which is taken modulo n repeats. For example, the sequence of Fibonacci modulo 5 is given as follows:
0 1 1 2 3 0 3 3 1 4 0 4 4 3 2 0 2 2 4 1 0 0 1 1 2 3 ...
This sequence has period 20, thus the Pisano period is $\pi(5) = 20$.
A Pisano period can be analyzed depending on its condition of being minimal or not.
Firstly, mod N of Pisano period is calculated. Then, aliquot of the Pisano period is determined, and all divisors except 1 are calculated. Starting with the largest divisor, all the successive divisors are tested whether they satisfy the equation or not. On the condition of value satisfying the equation, it is considered as new period and it returns to aliquots of the periods. On the contrary situation, aforementioned values among with its factor is discarded, and the process will be carried out by testing of the smaller factors. Therefore, it is worth to study1 the relationship between the period of Arnold's CAT map and the Pisano period of the Fibonacci sequence. From the connection between the matrix F and the matrix A if follows that the period of Arnold's CAT map will be exactly half of the Pisano period for all $N \geq 3$ [17].

5. Application of ACM to an Image Encryption

In this part two cases are considered; firstly an image having 21×21 dimension of pixels is used to present the readers a basic understanding of the ACM. Secondly, a 256×256 matrix associated with another image is used to analyze the period distribution of the CAT map.

Fig. 3. Peace Symbol



original image

Case 1:
A black and white peace symbol which is given in Fig. 3 is considered in order to show how iteration of CAT transformation is achieved in 2-dimensional CAT map.

$$\begin{pmatrix}
1&1&1&1&1&1&0&0&0&0&0&0&0&0&0&1&1&1&1&1&1\\
1&1&1&1&1&1&0&0&0&0&0&0&0&0&0&1&1&1&1&1&1\\
1&1&1&1&1&1&0&0&0&0&0&0&0&0&0&1&1&1&1&1&1\\
1&1&1&0&0&0&1&1&1&0&0&0&1&1&1&0&0&0&1&1&1\\
1&1&1&0&0&0&1&1&1&0&0&0&1&1&1&0&0&0&1&1&1\\
1&1&1&0&0&0&1&1&1&0&0&0&1&1&1&0&0&0&1&1&1\\
0&0&0&1&1&1&1&1&1&0&0&0&1&1&1&1&1&1&0&0&0\\
0&0&0&1&1&1&1&1&1&0&0&0&1&1&1&1&1&1&0&0&0\\
0&0&0&1&1&1&1&1&1&0&0&0&1&1&1&1&1&1&0&0&0\\
0&0&0&1&1&1&1&1&1&0&0&0&1&1&1&1&1&1&0&0&0\\
0&0&0&1&1&1&1&1&1&0&0&0&1&1&1&1&1&1&0&0&0\\
0&0&0&1&1&1&0&0&0&1&1&1&0&0&0&1&1&1&0&0&0\\
0&0&0&1&1&1&0&0&0&1&1&1&0&0&0&1&1&1&0&0&0\\
0&0&0&1&1&1&0&0&0&1&1&1&0&0&0&1&1&1&0&0&0\\
1&1&1&0&0&0&1&1&1&0&0&0&1&1&1&0&0&0&1&1&1\\
1&1&1&0&0&0&1&1&1&0&0&0&1&1&1&0&0&0&1&1&1\\
1&1&1&1&1&1&0&0&0&0&0&0&0&0&0&1&1&1&1&1&1\\
1&1&1&1&1&1&0&0&0&0&0&0&0&0&0&1&1&1&1&1&1\\
1&1&1&1&1&1&0&0&0&0&0&0&0&0&0&1&1&1&1&1&1
\end{pmatrix} \tag{17}$$

Each pixels of the Peace symbol are converted to a 21×21 matrix, by assigning the number "1" to "white" pixels and the number "0" to "black" pixels. The resultant matrix for this image is given in (17).
The evolution of ACM is carried out by the following three calculations:
Firstly, each entries of matrix are multiplied by the ACM matrix of the (3). Secondly, the resultant matrix is normalized. Lastly, each entries of the resultant matrix are multiplied by the ACM matrix. These steps are implemented continuously in order to reach the original image.

Accordingly, when the transformation is applied to the matrix given in (17), the original image is re-obtained in the 8^{th} step. The resultant image after the transformation for each step is shown in Fig. 4.

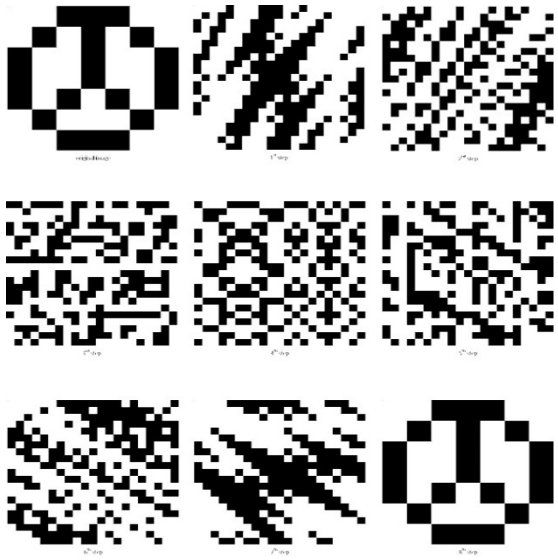


Fig. 4. The peace symbol with a 21×21 matrix.

Case 2:

For the second case, a grey scale 512×512 pixels of Lena picture is used to analyze the CAT map. The picture of Lena has been utilized into 256×256 pixels by Matlab®. The same calculation steps given in Case 1 are used for the CAT transformation. The initial picture reappeared after the 192^{th} step of transformation. The evolution of Lena's picture by using the CAT map is displayed in Fig. 5.

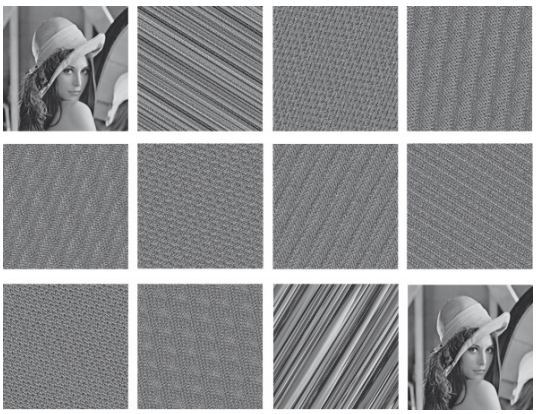


Fig. 5. The evolution of Lena's picture with a 256×256 matrix.

The relationship between the period of ACM and the dimension is discussed by taking into account of the results obtained in Case 1 and Case 2. The graph of period and dimension is given in Fig. 6. It is found that there is no a linear linkage between the number of period and the dimension.

On the other side, the results in Fig. 6 have an agreement with an upper bound of the period of the work done by Dyson and Falk who found the following relationship [7]:

$N = 2.5^k \ \rightarrow \ \psi_A(N) = 3N$

$N = 5^k \ or \ N = 6.5^k \ \rightarrow \ \psi_A(N) = 2N$

Others $\psi_A(N) \leq \frac{12}{7} N$

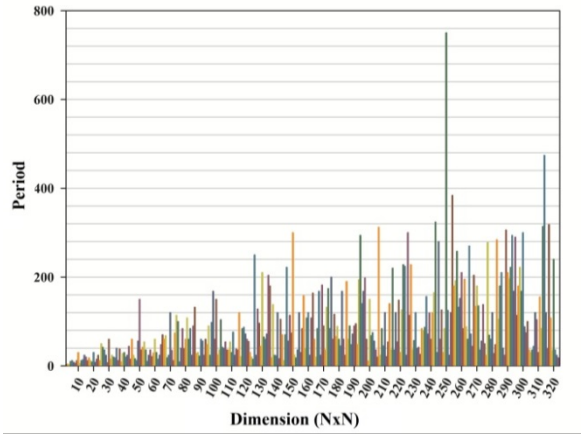


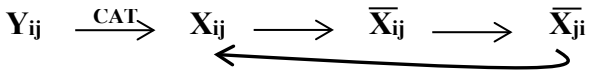
Fig. 6. A comparison of the dimension and the period of ACM

5.1. Proposed Algorithm

A new algorithm is developed to avoid the security problem driven by the upper bound of ACM. The algorithm can be described as the following steps:

i. The obtained data is assigned to the $N \times N$ dimensional two matrices of X and Y.
ii. The CAT map in (4) is applied to the matrix X.
iii. The transpose of the matrix X is calculated.
iv. Step ii and Step iii is repeated until to obtain the matrix Y.

The diagram of the proposed algorithm is displayed as follows:



Since the transpose of the matrix is calculated after each transformation. The period of the proposed algorithm is generally higher than the period of the usual CAT map. Since, more transformations are used in the proposed algorithm to reach the original data, it requires more calculations then the usual CAT map. As a result, more calculations yield in more transformations to get the original data. Therefore, the period of the transformation is increased. Additionally, the period of CAT map has an upper bound but period of the proposed algorithm grows exponentially. Furthermore, periods of the proposed algorithm display a sequence of relations as follows:

$N = 2^n \ \rightarrow \ \psi_A(N) = 2^{n+1}$

$N = 3^n \ \rightarrow \ \psi_A(N) = 16.3^{n-1}$

$N = 5^n \ \rightarrow \ \psi_A(N) = 24.5^{n-1}$

$N = 7^n \ \rightarrow \ \psi_A(N) = 12.7^{n-1}$

Table 1. Periods of usual CAT map and the proposed algorithm

Mod	N																						
	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	
C	3	4	3	10	12	8	6	12	30	5	12	14	24	20	12	18	12	9	30	8	15	24	
P	4	16	8	24	16	12	16	48	24	48	16	56	12	48	32	32	48	80	24	48	48	44	
	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	
C	12	50	42	36	24	7	60	15	24	20	18	40	12	38	9	28	30	20	24	44	15	60	
P	16	120	56	144	24	40	48	60	64	48	32	24	48	152	80	112	48	20	48	176	48	48	

A comparison of the period of usual CAT map and of proposed algorithm for CAT map is displayed in Table 1. The values of C represent the period of ACM and the values of P represent the period of the proposed algorithm.

6. Results and Discussion

In the image encryption of the CAT map, increase in the value of N will boost the encryption. However, the steps of CAT map transformation don't have any direct relation with increasing in the value of N. Accordingly, increasing the value of N does not result in complexing of the encryption. Moreover, a relationship with dimension and period in ACM is given in Fig. 6. It shows that the dimension N is not proportional to the period of ACM.

Furthermore, the proposed algorithm is applied to a 256×256 pixels image of Lena picture and it is observed that the original picture is reappeared after the 512^{th} step. In the case of the application of the usual CAT map to same pixel size of Lena's picture, it has been seen that the original picture is obtained after the 192^{th} step. This result suggests that the period of proposed algorithm is greater than the period of usual ACM. In order to avoid the period problem, a new algorithm has been established in Section 5.1. The proposed algorithm uses a safer encryption without increasing the value of N.

It can be easily inferred from the Table 1 that the period of the proposed algorithm is bigger than the period of usual ACM. This shows that having bigger number of period results in more secure encryption. For that reason, without increasing the value of N more efficient encryption can be obtained. Additionally, small value of N yields less calculations. Calculation cost will be much more less with the small value of N.

The algorithm is applied to images by re-dimensioning of the $N \times N$ matrix. Since the original image is redimensioned to the unknown N, it cannot be easy to predict the value of N. Finally, the value of N for decryption should be known in order to implement this method. Even after obtaining and identifying the value of N, the decryption will not be straightforward, since the CAT map is applied together with a proposed algorithm.

Generally, an encrypted data needs to be decrypted. However, in ACM a decryption can be made through a certain repetition of the transformations. From this point of view, the proposed algorithm uses ACM for encryption but the decryption is obtained through the value of N.

When the values of p and q are changed in usual CAT map in (7), the period will also change and the security can be ensured partially since the values of p and q are arbitrary.

The security can be increased by sending the information about in which step the algorithm is, separately.

7. Conclusion

Recently, with increasing of the usage of digital media, the need to secure all transferred data gained a big importance. For that reason, certain algorithms are proposed such as Arnold's CAT Map. The ACM can be applied to a wide range of areas which includes encryption of images. Important data can be transferred by using ACM in more secure way. In this work, Arnold's CAT Map is studied and a proposed algorithm is introduced.

The period of encrypted data is important by the means of calculation cost. Therefore, the periodicity of two algorithms is discussed and compared. There e is no linear relationship between dimension and period of ACM. However, the security can be enhanced by using an additional function in the algorithm. Since, the proposed algorithm uses transposes matrix of the data it yields the bigger period. The period of ACM has an upper bound while the period of proposed algorithm is growing exponentially.

Acknowledgments

The authors would like to acknowledge Ege University Research Foundation (Project No: 16 /FEN/ 057) for their financial support.

References

[1] J. Franks. "Anosov diffeomorphisms" in global analysis, proc. Sympos, Pure math, American Mathematical Society, vol. 14, pp. 61-93, 1968.

[2] Edward R. Scheinerman, "Invitation to Dynamical Systems," Dept. of Math. Sciences, Johns Hopkins University, USA, 1996.

[3] Timur Karacay, "Determinizm ve Kaos," 2004.

[4] M.A. Partnof and K. Crum, "Chaos and Arnold's cat map," 2004.

[5] V.I. Arnold and A. Avez, "Ergodic Problems of Classical Mechanics," Benjamin, 1968.J. Franks. "Anosov diffeomorphisms" in global analysis, proc. Sympos, Pure math, American Mathematical Society, vol. 14, pp. 61-93, 1968.

[6] J.P. Keating, "Asymptotic properties of the periodic orbits of the cat," Nonlinearity, vol. 4, pp. 277-307, 1991.

[7] F.J. Dyson and H. Falk. "Period of a discrete cat mapping," The American Mathematical Monthly, vol. 99, pp. 603-614, 1992.

[8] W. Chen, C. Quan, and C.J. Tay, "Optical color image encryption based on Arnold transform and interference method," Optics Communications, vol. 282, pp. 3680-3685, 2009.

[9] Z. Liu, L. Xu, T. Liu, H. Chen, P. Li, C. Lin, and S. Liu, "Color image encryption by using Arnold transform and color-blend operation in discrete cosine transform domains," Optics Communications, vol. 284, pp. 123-128, 2011.

[10] Xiangjun Wu, Haibin Kan, and Jurgen Kurths, "A new colour image encryption scheme based on DNA sequences and multiple improved 1d chaotic maps," Applied Soft Computing, vol. 37, pp. 24-39, 2015.

[11] A. Soleymani, J.Nordin, and E. Sundararajan, "A chaotic cryptosystem for images based on Henon and Arnold cat map," Hindawi Scientic World, pp. 1-21, 2004.

[12] Lu Xu, Zhi Li, Jian Li, and Wei Hua, "A novel bit-level image encryption algorithm based on chaotic maps," Optics and Lasers in Engineering, vol. 78, pp. 17-25, 2016.

[13] Necla Kircali Gursoy and Urfat Nuriyev, "Some Inequalities for Algebra of Fractions and Its Applications," Advanced Math. Models & Applications, vol. 1 pp. 1-13, 2016.

[14] Ahmed M. Elshamy, Fathi E. Abd El-Samie1, Osama S. Faragallah, Elsayed M. Elshamy, Hala S. El-sayed, S. F. El-zoghdy, Ahmed N. Z. Rashed, Abd El-Naser A. Mohamed, and Ahmad Q. Alhamad, "Optical image cryptosystem using double random phase encoding and Arnold's Cat map," Opt Quant Electron, Springer, vol. 48:212, 2016.

[15] Yueping Li, Chunhua Wang, and Hua Chen, "A hyper-chaos-based image encryption algorithm using pixel-level permutation and bit-level permutation," Optics and Lasers in Engineering, vol. 90, pp. 238-246, 2017.

[16] Chanil Pak, and Lilian Huang, "A new color image encryption using combination of the 1D chaotic map," Signal Processing, vol 138, pp. 129-137, 2017.

[17] Fredrik Svanstrom, "Properties of a Generalized Arnold's Discrete Cat Map," M.S. thesis, Dept. Math., Linnaeus University, Sweden, 2014.

[18] F. Chen, K. Wong, X. Liao, and T. Xiang, "Period distribution of generalized discrete Arnold cat map for n=p^e.," Transactions on Information Theory, vol. 58, pp. 445-452, 2012.