Iraqi Journal for Computer Science and Mathematics

Journal Homepage: http://journal.esj.edu.iq/index.php/IJCM

e-ISSN: 2788-7421 p-ISSN: 2958-0544

Auto–Transition in RADG based on chaotic System

Laith M. Kadhum[1,2]*, Ahmad Firdaus[2]*, Mohamad Fadli Bin Zolkipli[2], Syifak Izhar Hisham[2], Luhur Bayuaji[2], Mohd Faizal Ab Razak[2]

[1] Faculty of Engineering, University of Kufa, Najaf, ,
Najaf, 54001, Iraq

[2] Faculty of Computing, Universiti Malaysia Pahang,
26600 Pekan, Pahang, Malaysia

DOI: https://doi.org/10.52866/ijcsm.0000.00.00.000

Received 00 Month 2000; Accepted 01 Month 2000; Available online 02 Month 2000

ABSTRACT:

The RADG (Reaction Automata Direct Graph) cryptosystem is the automata direct graph and reaction states combination. The classical RADG does not require key exchange (keyless), or agreement between users just the design of RADG, which is static. The RADG algorithm with keys has two agreements between users, one is on the keys, and other is a design of RADG. The RADG design depends on states and transitions between them, since transitions between states are static transitions, or dynamic transitions have agreement between users to determine the type of state (Jump state, Reaction state) of RADG algorithm with keys, and the transition between states must cover each states scenario of RADG design .This article presents algorithm called (Auto- Transition Function (ATF)), which merge properties of RADG algorithm with chaotic system to obtain on transitions between states are automatic. The parameters of ATF are chaotic initial value, parameter of chaotic function, and characteristics of RADG, then ATF is an auto creation of transitions among all states in RADG, and it satisfies each scenario of RADG design.

Keywords chaotic system, cryptography, RADG, Block Cipher, Chaotic tent map, Auto-Transitions function, ATF for RADG.

1. Introduction

In recent years, chaotic systems have been extensive studies in many different fields of science, such as medicine, engineering, mathematic, economic, biology and chemistry [1][2][3]. The chaotic systems are very interesting phenomenon in systems of nonlinear dynamical [4][5] . A chaotic system have unique properties such as high sensitivity on initial conditions and unpredictability [6][7], These properties can play important role in constructing transition function between states in RADG cryptosystems [8].

Reaction Automata Direct Graph (RADG) is based on reaction states (R) and Automata Direct Graph (ADG), where R used to reduce and increase the random expectations, and ADG is a direct graph has states, and transitions corresponding verities, and edges in the graph with respectively, the relation between states in RADG dependent on transitions between them. The classic RADG (keyless) depends on the static design and characteristics by utilizing in the private communication, therefore design of RADG and transitions between states are static [9]. In [8] proposed a chaotic RADG, which is combined logistic map with RADG to obtain dynamic transitions between states, dynamic transitions not cover all transitions between states, which have more than one component of RADG digraph, and each state determined by agreement between users, moreover dynamic transitions may have loop in some of standard states. in [10], the dynamic transitions between states in RADG are sequence of addresses depended on McEliece encryption of previous address ,with reverse ,and negation of cipher-previous-address , to select the next address, that means there are no warranty to cover all

*Corresponding author: laithmr@uokufa.edu.iq , firdausza@ump.edu.m

states in ME-RADG (McEliece-RADG), and design of RADG scenario. In [11] improved design of RADG by developing single Reaction states into Multi-Reaction called Multi-Reaction Automata Direct Graph(MRADG), which used transition function between states, the transition function used two keys between communications parties, one is public key and other secondary key, as well as have agreement between parties to determine reaction states and jump states, therefore transition function in MRADG added more agreements between parties communication, and there is no guarantee the design covering all states of MRADG.
In this article presents Auto- Transition Function (ATF), which is solved problems of transitions between states in RADG design (with keys, without keys). ATF provides a simple transitions between states, which covers all the states in RADG design, as well as not addition more agreements between parties communication, therefore it satisfies scenario of RADG design. ATF depends on the initial value of chaotic system, parameter of chaotic system, and characteristics of RADG design. ATF uses the chaotic tent map is utilized for producing chaotic sequences. The chaotic tent map is an iterated function that forms a dynamic system of discrete time, which demonstrates a chaotic dynamical behavior [12]. Chaotic tent map expression is presented by [13]:

$$x_n = \begin{cases} \mu x_{n-1} & x_{n-1} < 0.5 \\ \mu(1 - x_{n-1}) & Otherwise \end{cases} \qquad (1)$$

Where, $Xn \in [0, 1]$, for $n \geq 0$. This map transforms the interval [0,1] on itself also include just a parameter of control μ , respectively, where $\mu \in [0, 2]$.

2. Reaction Automata Direct Graph (RADG)

RADG design can be presented by set of tuples (sextuple) as (R; Q; Σ; Ψ; J; T) where: R represent finite set of reaction states, Q represent finite set of standard states, Σ represent finite set of input data, Ψ represent finite set of output transitions, J represent finite set of jump states (which is subset of Q), and T represent transition function, which have (state address, message bit) [14].The encryption process of RADG depends on (n, m, k and λ), where $n = |Q|$, such ($n \geq 2$), $m = |R|$, k is the number of jump states ($k \leq \lfloor \frac{n}{2} \rfloor$), and λ represent the number of values in each state except jump states, jump states has not any value, it only transmits from one state to another state [9].

The encryption process in RADG starts by selecting a random state from Q-set (expect jump states), if Q state lead to jump state, then select a random state from R states, after that back to Q-set to continue encryption process [9]. The state in RADG design consists from (state address and values of state). In Fig.1, assume $\lambda = 2$, then $\sum = \{0, 1\}$ (this means the state have state address and two values).Example 2.1 illustrates how RADG method is working.

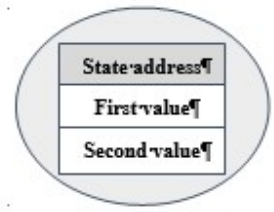

Figure1 Representation of the state

Example 2.1:

If n = 5, m = 2, k = 1,assume $\lambda = 2$, then $\sum = \{0, 1\}$,and $\Psi = \{11, 12,13,14,15,16,17,18,19,20,21,22\}$.
Let state numbers4 and 5 are states of R (set of reaction states)as well as the number of state 0,1,2 ,3 and6 are states of Q (set of standard states), the state number 6 is J(jump state) in Q sets (since k=1) In this example, assume the plain text is 0001, which encrypts by using RADG algorithm.

Suppose transitions between states are static and the RADG algorithm selects state 0 as first state with first bit of plain text is 0 , then the transition function will be as the following :
Step1: T (0,0) = (2,11)

- T (0,0): The first value is a state address which is 0 and the second value is the first bit of plain text which is 0.
- (2,11): this means message 0 gives 11 as cipher and moves to state 2 by transition drawing.

Step2:T(2,0)=(3,13)

- T (2,0): The first value is a state address which is 2 and the second value is the second bit of plain text which is 0.
- (3,13): this means message 0 gives 13 as cipher and moves to state 3 by transition drawing.

Step3:T(3,0) =(4,17)

- T (3,0): The first value is a state address which is 3 and the second value is the third bit of plain text which is 0.
- (4,17): this means message 0 gives 17 as cipher and moves to jump state which is 6, then jump state selects a random state from reaction states , suppose jump state selects state 4.

Step4:T(4,1) =(1,20)

- T (4,1): The first value is a state address which is 4 and the second value is the fourth bit of plain text which is 1.
- (1,20): this means message 1 gives 20 as cipher and moves to state 1 by transition drawing.

The cipher text is 11,13,17 and 20 respectively.

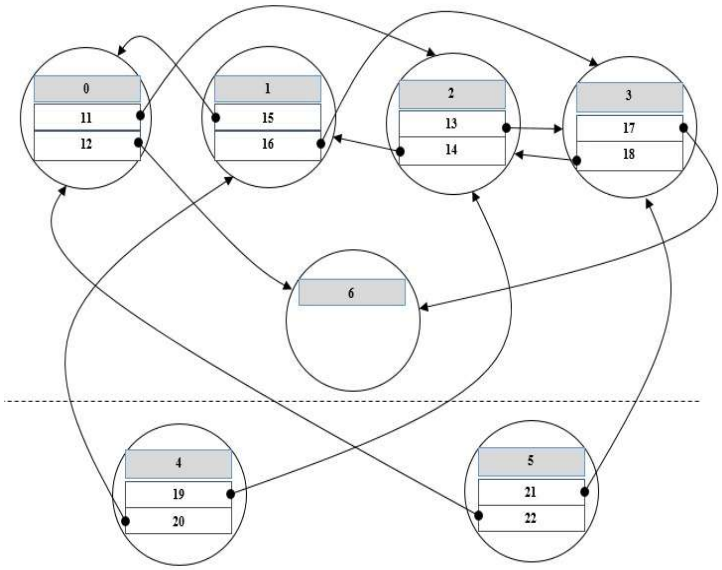

Figure 2 **Implementation of RADG algorithm**

3. Auto-Transition Function

The purpose of the Auto-Transition Function (ATF) is to make transitions between states in RADG design generated automatically by using chaotic tent map. ATF satisfies scenario of RADG design, which covers all states in RADG design, ATF is depended on keys (number of states in Q set, number of states in R set, number of states in J set (jump state) , the number of transitions from Q to J which denoted by ω, the initial value of chaotic map function , and the parameter of chaotic map) of the RADG cryptography between the sender, and the receiver, these keys will be changed with modification of ATF, keys might depend on the chaotic sequences (Tent, logistic, Gaussian, …) map start from x_0, with parameters depended on the chaotic map. The chaotic system used in this article is a chaotic tent map. The chaotic tent map created sequence of values from (Eq.1). where (x_0,x_1,x_2,…) depend on recurrence relation of x_n and the value of the parameter μ (within 0 and 2), the next value x_{n+1} in the interval [0, 1], the iterating a point start from x_0 initial value in [0,1] gives rise to a sequence (x_1,x_2, …).

ATF is to find the next state from state s, and the order value v in state s, with tent sequence start from x_0, the parameter $0<\mu<2$, and fixed value states λ , ATF has three components as the following:

$$ATF(s,v)=\begin{cases} r+\alpha-1 & (\lambda s+v)\in J', and\ j_r=\lambda s+v \\ f(x_{\lambda s+}\ ,n,k,\tau) & s\le n-k-1, and\ (\lambda s+v)\notin J' \\ \lfloor x_{\lambda s+v}\,(n-k)\rfloor & Otherwise \end{cases} \quad (2)$$

Where *s* denoted to the address of state, *v* denoted to the order value in the state *s*, n the number of standards states in set Q, *k* the number of jump states, λ is a number of values in each states of RADG, *m* the number of reaction states in set R, and τ the number of values in RADG design where

$$\tau=\lambda(n+m-k) \quad (3)$$

in (Eq.2), the value $x_{\lambda s+v}$ belong to the set $\{x_0,x_1,\dots,x_{\tau+k-1}\}$ which generate from (Eq.1), where $s=0,1,\dots,\alpha-1,$ and $v=0,1,\dots,\lambda-1$.
The number of states in RADG except jump states denoted by α, where

$$\alpha=(n+m-k) \quad (4)$$

The first component of (Eq.2), is next jump state, where (*r*=1,2,….,*k*), α is number of states in RADG except jump states, and $(\lambda s+v)\in J'$, where $J'\subseteq V_Q$ such that $J'=\{j_1,\dots,j_k\}$, and j_i a random *k*-values between 0, and $\lambda(n-k)-1$, denoted by V_Q , i=1,2,…,*k*.

The J' set is a subset of order values of V_Q selected a random states under chaotic tent sequence from (x_τ to $x_{\tau+k-1}$).
To calculate the J' set apply the fallowing steps:

1- change (x_τ to $x_{\tau+k-1}$) to integer number by the following equation :

$$A=\{a_i \mid a_i=\lfloor\lambda\,(n-k)x_{i+\tau-1}\rfloor,\ x_{i+\tau-1}\in X, and\ \ i=1,2,\dots,k\} \quad (5)$$

Where $X=\{\ x_i|x_i\ are\ Tent\ value\ map\ i=0,1,\dots,\tau+k-1\}$

The purpose of finding *A* is to determine the next state from V_Q to jump state

2- To ignore the reparation that happen in *A*. find a sequence of P and B ,which used to choose different nest state from V_Q to jump state , where P and B have integer elements define by :

$$P=\{p_i|p_i=1, if\ a_i\ \in E, otherwise\ p_i=0, E=\{a_1,\dots,a_{i-1}\}, 1\le i\le\ k\} \quad (6)$$

$$B=\{b_j \mid b_j\notin A, 0\le b_j\le\ |V_Q|-1, j=1,2,\dots,|V_Q|\} \quad (7)$$

Then the sequence $j_1,j_2,\dots,j_k$ of distinct integer number is defined by:

$$J'=\{j_i|j_i=(1-p_i)a_i+p_i b_{\sum_{j=1}^{i}p_j}\ ,\ \ a_i\in A, p_i\ \in P, and\ b_{\sum_{j=1}^{i}p_j}\in B\}$$

Then

$$J'=\{j_1,\dots,j_k\},\ \ 0\le\ j_i\le\lambda(n-k)-1,\ \ \text{i}=1,2,\dots,\text{k} \quad (8)$$

This Example explains how to find J' set:

Let *n*=15, m=9, *k*=7, λ=2, x_0=0.137, and μ=1.98, and x_{34} to x_{40} are

0.4453 0.8817 0.2342 0.4637 0.9180 0.1623 0.3213

then τ=34 from (Eq. 3), α=17 from (Eq. 4) , *A*={7,14,3,7,14, 2 ,5} from (Eq. 5), *P*={0,0,0,1,1,0,0} from (Eq.6) and *B*={0 ,1, 4 , 6 , 8 , 9 ,10 ,11,12 ,13,15} from (Eq.7)

Then J'={7,14 ,3 ,0 ,1 ,2 ,5 } from equation (8)

The second component of (Eq. 2), is the next state from set $V_Q = \{0,1,\cdots,\lambda(n-k)-1\}$ to same set $V_Q = \{0,1,\cdots,\lambda(n-k)-1\}$, if $s \le n-k-1, and\ (\lambda s+v) \notin J'$, its under the function of four independent parameters $x_i, n, k, and\ \alpha$, such that the function $f(x_i,n,k,\alpha)$ is define by:

$$f(x_i,n,k,\alpha) = \begin{cases} \lfloor \alpha + k y_i \rfloor & x_i < \delta \\ (\lfloor x_i\ (n-k) \rfloor + 1)\ mod\ (n-k) & if\ \lfloor x_i\ (n-k) \rfloor = \left\lfloor \frac{i}{\lambda} \right\rfloor \\ \lfloor x_i\ (n-k) \rfloor & otherwise \end{cases} \quad (9)$$

The first component of (Eq.9), is to make extra next state from V_Q to jump state.

Where δ is much less than one (δ <<1), the value (δ) dependent on the numbers *n, k,* λ , $\{x_i\}_{i=1}^{\lambda(n-k)}$. The extra next state from V_Q to jump state denoted by ω , where $k \le \omega \le \frac{\lambda(n-k)}{2}$,
and $|V_Q| = \lambda(n-k)$.

The value (δ) calculates by following equation:

$$\delta = \frac{(\min^{(\omega-k)}\{x_i\}_{i=1}^{|V_Q|}) + (\min^{(\omega-k+1)}\{x_i\}_{i=1}^{|V_Q|})}{2} \quad (10)$$

The above (Eq.10) means that when sorted the set $\{x_i\}_1^{|V_Q|}$ to the set $\{x_i'\}_{i=1}^{|V_Q|}$, such that $x_i' < x_j'$, and *i*<*j* for all *i,j*=1,2,…,$|V_Q|$, then $x'_{\omega-k} = \min^{(\omega-k)}\{x_i\}_{i=1}^{|V_Q|}$.

Example to calculate the value (δ) : let *n* = 7, λ=2, *ω*=4, *k*=2 , then $|V_Q| = 10$

$$\{x_i\}_{i=1}^{10} = \{0.3370, 0.6673, 0.6588, 0.6755, 0.6425, 0.7079, 0.5783, 0.8350, 0.3267, 0.6469\}$$

$$\{x_i'\}_{i=1}^{10} = \{0.3267, 0.3370, 0.5783, 0.6425, 0.6469, 0.6588, 0.6673, 0.6755, 0.7079, 0.8350\}$$

$$x_2' = x_1 = \min^{(2)}\{x_i\}_{i=1}^{10} = 0.337$$

$$x_3' = x_7 = \min^{(3)}\{x_i\}_{i=1}^{10} = 0.5783$$

$$\delta = \frac{0.337 + 0.5783}{2} = 0.4577$$

The first component of (Eq.9), if $x_i < \delta$, where x_i belong to the set $\{x_0, x_1, \dots, x_{|V_Q|-1}\}$, and the set that satisfy $x_i < \delta$ denoted by $J^{(\omega-k)}$, such $J^{(\omega-k)} = \{x_1', x_2', \dots, x'_{\omega-k}\}$, $x_i' < x_j'$, $i < j$, $i,j = 1,2,\dots,\omega-k$, where $J^{(\omega-k)} \subseteq \{0,1,\dots,|V_Q|-1\}$.

The problem of the set $J^{(\omega-k)}$ is biased to the interval is less than δ, that is unbalance because it must be in the interval (0,1), then by the following steps convert the set $J^{(\omega-k)}$ (each element in $J^{(\omega-k)}$ belong to the interval $[x_1', x'_{\omega-k}]$) to the interval $(\gamma, 1-\gamma)$ such that:

1- $\gamma = \frac{\min\{x'_{i+1} - x'_i\}}{2}$ i=0,1,2,…, ω-k-1 , where $x_0' = 0$. (11)

Then to convert interval $[x_1', x'_{\omega-k}]$ to interval $[\gamma, 1-\gamma]$ by using equation of a straight line as the following:

2- $y_i = \frac{1-2\gamma}{x'_{\omega-k}-x'_1}(x_i - x'_1) + \gamma$ (12)

To calculate y_i suppose $J^{(\omega-k)} = \{ x'_1 = 0.3267, x'_2 = 0.3370 \}$, then $\gamma = 0.0052$ from (Eq.11)

Then

$$y_1 = 0.0052 \, , y_7 = 0.9948$$

If ω =k then $J^{(\omega-k)} = J^{(0)} = \phi$, which mean there is not extra next state from V_Q to jump state .

The second component of (Eq.9), if next state $\lfloor x_i\ (n-k) \rfloor$ is the same state $s = \left\lfloor \frac{i}{\lambda} \right\rfloor$, or $\lfloor x_i\ (n-k) \rfloor = \left\lfloor \frac{i}{\lambda} \right\rfloor$, then next state $(\lfloor x_i\ (n-k) \rfloor + 1)\ mod\ (n-k)$ in V_Q, where $V_Q = \{0,1,\cdots,\lambda(n-k)-1\}$, where the purpose of second component in (Eq.9), is to ignore the loop in states.

The third component of (Eq.9) is next state with otherwise of first, and second components.

The third component of (Eq.2) is next state from set V_R to set V_Q , where $V_R = \{\lambda(n-k), \lambda(n-k)+1, \cdots, \lambda(n+m-k)-1\}$ and $V_Q = \{0,1,\cdots,\lambda(n-k)-1\}$

3.1 Algorithm of ATF:

Input :

Chaotic data : x_0 ,μ.

RADG data : n, m, k, λ, ω.

Condition for jump state: $k \le \omega \le \frac{\lambda(n-k)}{2}$

Output:

Array D from 1 to λ* (n+m-k)

Process:

τ = λ* (n+m-k);

α = n+m-k;

V_{nk}=n-k;

$|V_Q|$= λ*V_{nk};

Lx= τ+k;

Set the tent chaos sequence x_0 , x_1,…, $x_{\tau+k-1}$;

$$\delta = \frac{(\min^{(\omega-k+1)}\{x_i\}_{i=0}^{|V_Q|-1}) + (\min^{(\omega-k)}\{x_i\}_{i=0}^{|V_Q|-1})}{2}$$

D(i)=[x_{i-1}*V_{nk}], i=1,2,.., τ;

$J^{(\omega-k)} = \phi$

$\gamma = \frac{\min\{x_j - x_i\}}{2}$, such that $x_i, x_j < \delta$

if $x_{i-1} < \delta$

$$y_i = \frac{1-2\gamma}{\min^{(\omega-k)}\{x_i\}_{i=0}^{|V_Q|-1} - \min^{(1)}\{x_i\}_{i=0}^{|V_Q|-1}}\left(x_i - \min^{(1)}\{x_i\}_{i=0}^{|V_Q|-1}\right) + \gamma$$

D(i)=$\lfloor \alpha + k\ y_i \rfloor$i=1,2,.., $|V_Q|$;

$J^{(\omega-k)} = J^{(\omega-k)} \cup \{D(i)\}$;

end

if$\left\lfloor \frac{i-1}{\lambda} \right\rfloor$ ==D(i)

D(i)=(D(i)+1) mod V_{nk} i=1,2,.., $|V_Q|$;

End

z(i)= $x_{\tau+i-1}$ i=1,2,..,k;

z(j)=z(1), $j=k+1,\ldots, |V_Q|$
Dk1$(i) = \lfloor z(i) * |V_Q| \rfloor$ i=1,2,…,k,k+1, …, $|V_Q|$
B array is different between Dk1, and 0,1,…, $|V_Q|$-1
P array of zero-one , one if repeat element in Dk1, otherwise zero.
k=0;
for i=1,2,…, $|V_Q|$
if $p(i)$==1 then
$k=k+1$;Dk2(i)=B(k);
else
Dk2(i)=Dk1(i)
end
Dk(i)= Dk2(i) i=1,…,k
D(Dk(i)+1)= α+i-1 ; j(i)= Dk(i)+1 ; i=1, …, k
$J' = \{j(1), \ldots, j(k)\}$, withDifferent values of $J' \cup J^{(\omega-k)}$
End Process

3.2 Example of ATF

Suppose n=8, m=4, k=3, λ=2 ,then ∑ ={0, 1}, x_0=0.74, μ=1.98, and ω=3

1- Find number of values in all states from (Eq.2), τ = λ (n+m-k) =18
2- Generating sequence of x_i from (Eq.1), such as $xi = \{x_0, x_1, \ldots, x_{\tau+k-1}\}$, where x_i (i=0,1,…,18, 19,20) under chaotic tent map are

Chaotic sequences under chaotic tent map										
x_0	x_1	x_2	x_3	x_4	x_5	x_6	x_7	x_8	x_9	x_{10}
0.7400	0.5148	0.9607	0.0778	0.1541	0.3051	0.6041	0.7839	0.4279	0.8471	0.3026
x_{11}	x_{12}	x_{13}	x_{14}	x_{15}	x_{16}	x_{17}	x_{18}	x_{19}	x_{20}	
0.5992	0.7935	0.4089	0.8096	0.3770	0.7465	0.5020	0.9861	0.0275	0.0544	

3- since $\omega = k$, then $J^{(\omega-k)} = J^{(0)} = \phi$, which mean there is not extra next state from V_Q to jump state
4- Calculate J' as the following to find next state from V_Q to jump state:
   - Generate chaotic sequence of x_i, where x_i =(x_τ to $x_{\tau+k-1}$) ,such x_i (i=18,19,20) are:

     x_{18}=0.9861 , x_{19}= 0.0275 ,x_{20}= 0.0544

   - Find A from (Eq.5), Then A= { 9, 0 , 0 },
   - To ignore the reparation of values that happen in A , finding P and B , where P={0,0,1} from (Eq.6), and B={1,2,3,4,5,6,7,8}from (Eq.7)

   Then J' : j_1=9, j_2=0, j_3=1, from (Eq.8)

5- Find number of states in RADG design (except jump states) from (Eq.4), then $\alpha = 9$.
6- Representation the states with their values, where each state in Q\J and R have values, the values of states are chaotic sequences and {0,1} because λ=2, where Q\J means standard states (except jump states), and R means reaction state. as the following table

State	State number	0		1		2		3		4	
Q\J	State value	0	1	0	1	0	1	0	1	0	1
	Chaotic sequences	0.7400	0.5148	0.9607	0.0778	0.1541	0.3051	0.6041	0.7839	0.4279	0.8471
State	State number	5		6		7		8			
R	State value	0	1	0	1	0	1	0	1		
	Chaotic sequences	0.3026	0.5992	0.7935	0.4089	0.8096	0.3770	0.7465	0.5020		

7- Converting the chaotic sequences to integer values by using $(\lfloor x_i\ (n-k) \rfloor)$. To get the next state. If the integer value of next state is same number of state then used the second component of (Eq.9) to ignore the loop in states.

State	State number	0		1		2		3		4	
Q\J	State value	0	1	0	1	0	1	0	1	0	1
	Next state	3	2	4	0	0	1	4	4	2	0
State	State number	5		6		7		8			
R	State value	0	1	0	1	0	1	0	1		
	Next state	1	2	3	2	4	1	3	2		

8- Finding jump state from the first component of (Eq.2) as the following

r+ α-1	Jump state
1+9-1	9
2+9-1	10
3+9-1	11

Sine J' is 9, 0, 1 corresponding for state number (s), and value of state (v), then the elements of J' lead to jump states as the following :

J'	State number (s)	Value of state(v)	r+ α-1	Jump state
9	4	1	1+9-1	9
0	0	0	2+9-1	10
1	0	1	3+9-1	11

9- Representation the table of transitions from state to the next state as the following

State	State number	0		1		2		3		4	
Q\J	State value	0	1	0	1	0	1	0	1	0	1
	Next state	10	11	4	0	0	1	4	4	2	9
State	State number	5		6		7		8			
R	State value	0	1	0	1	0	1	0	1		
	Next state	1	2	3	2	4	1	3	2		

The Graph Design of RADG by using ATF:

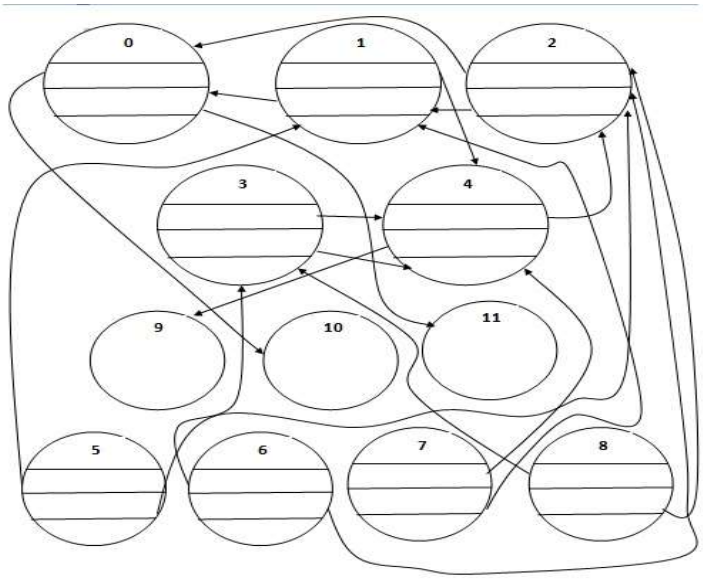

Figure 3 RADG Design Using Auto-Transition Function

3.3 Case Study:

Applying the ATF-Algorithm with input data n=360, m=215, k=20, λ=2, $x0$=0.4121, μ=1.97, and ω=30 then τ = λ (n+m-k) =1110, n-k=340, α=n+m-k=555, then description RADG design transition by the following graph:

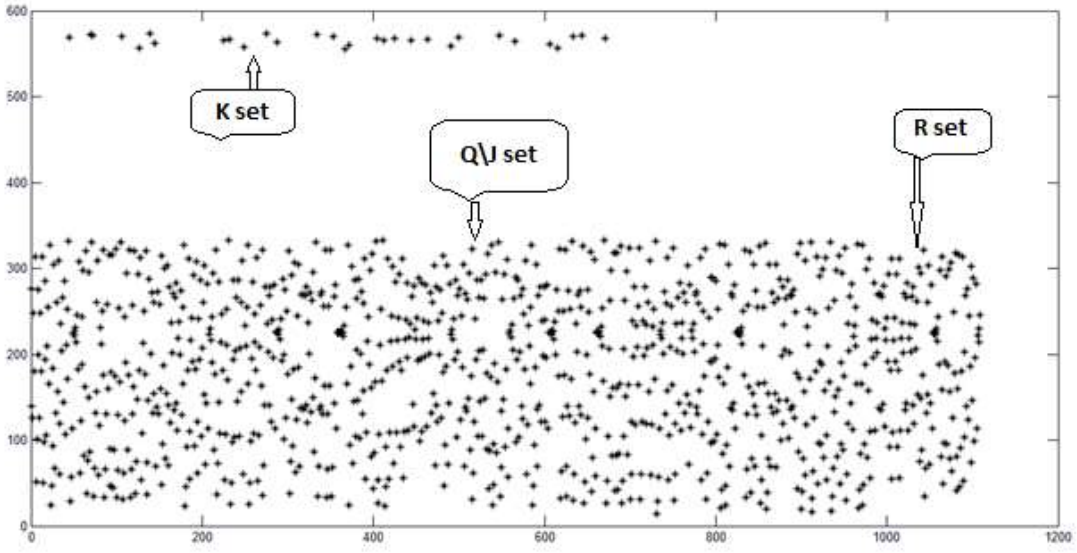

Figure 4 RADG states distribution (case study)

4. Analysis of ATF

The analysis of the power of ATF dependent on the sensitivity of different value of initial value of chaotic sequences, and parameter of chaotic tent map.

Let the values of initial value standard x_0=0.7459, μ=1.98 and comparison RADG design with other initial values 0.01, 0.02, …., 0.99, with same parameter μ=1.98 then the following figure Fig.5 describe the similarity with standard initial value x_0=0.7459, where n=30, m=15, k=12, λ=2, and ω=12

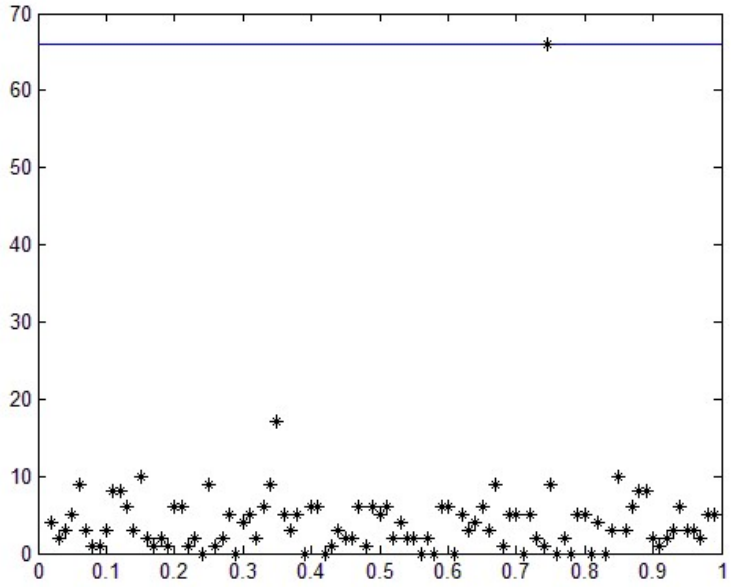

Figure 5 : The comparison RADG design at x0=0.7459, with 0.01, 0.02, 0.03, …, 0.99

Where initial value x_0=0.74 , and the comparison with transition RADG design with other initial values 0.741,0.742, …, 0.79, are greater than 0.74, then the following figure Fig.6 shows the similarity of values with standard initial value x_0=0.74

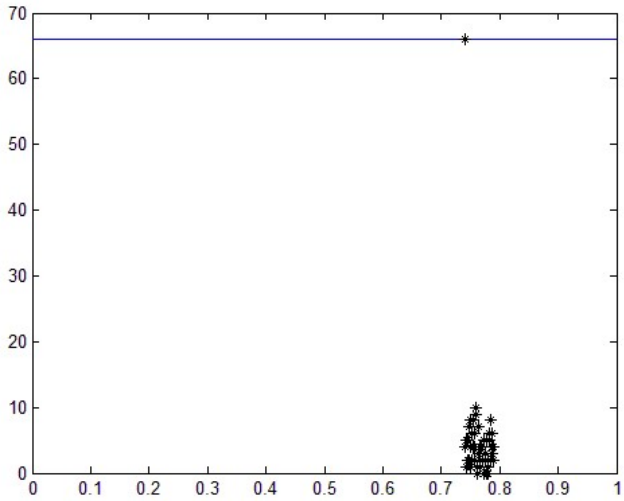

Figure 6 : The comparison RADG design at x0=0.74, with 0.0.741, 0.742, 0.743, …, 0.79

Where x_0=0.74 , and comparison RADG design of left standard value x_0=0.74 with the following values 0.6,0.601, …, 0.69. then the following figure Fig.7 shows comparison RADG design at x0=0.74, with 0.6,0.601, …, 0.69

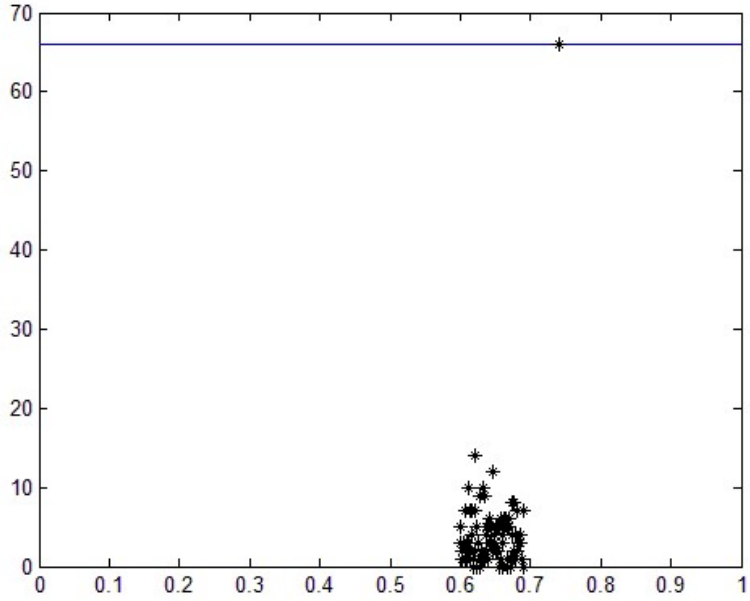

Figure 7 : The comparison RADG design at x0=0.74, with 0.6,0.601, …, 0.69

5. CONCLUSIONS

This paper proposes Auto-Transition Function (ATF), which salved problems of transitions between states in RADG design based on chaotic tent map. ATF satisfies scenario of RADG design, which covers the states in RADG design, as well as not addition more agreements between parties communication, ATF depends on keys (number of states in Q set , number of states in R set , number of states in Jump set, the number of transitions from Q to jump denoted by ω, the initial value of chaotic tent map function, and the parameter of chaotic tent map) of the RADG cryptography between the sender, and the receiver, these keys will be changed with other communication between them and can be modification of ATF.

ACKNOWLEDGEMENT

This work is funded by the collaboration matching grant between Kaneka Malaysia (UIC220830) and Universiti Malaysia Pahang (UMP) (RDU222410).

REFERENCES

[1] C. Li, G. Luo, K. Qin, and C. Li, "An image encryption scheme based on chaotic tent map," *Nonlinear Dyn.*, vol. 87, no. 1, pp. 127–133, 2017, doi: 10.1007/s11071-016-3030-8.

[2] M. S. Tavazoei and M. Haeri, "Comparison of different one-dimensional maps as chaotic search pattern in chaos optimization algorithms," *Appl. Math. Comput.*, vol. 187, no. 2, pp. 1076–1085, 2007, doi: 10.1016/j.amc.2006.09.087.

[3] N. K. Pareek, V. Patidar, and K. K. Sud, "Discrete chaotic cryptography using external key," *Phys. Lett. Sect. A Gen. At. Solid State Phys.*, vol. 309, no. 1–2, pp. 75–82, 2003, doi: 10.1016/S0375-9601(03)00122-1.

[4] Z. Wei, "Dynamical behaviors of a chaotic system with no equilibria," *Phys. Lett. Sect. A Gen. At. Solid State Phys.*, vol. 376, no. 2, pp. 102–108, 2011, doi: 10.1016/j.physleta.2011.10.040.

[5] N. Singh and A. Sinha, "Gyrator transform-based optical image encryption, using chaos," *Opt. Lasers Eng.*, vol. 47, no. 5, pp. 539–546, 2009, doi: 10.1016/j.optlaseng.2008.10.013.

[6] Z. Hua, Y. Zhou, and H. Huang, "Cosine-transform-based chaotic system for image encryption," *Inf. Sci. (Ny).*, vol. 480, pp. 403–419, 2019, doi: 10.1016/j.ins.2018.12.048.

[7] L. Liu and S. Miao, "A new image encryption algorithm based on logistic chaotic map with varying parameter," *Springerplus*, vol. 5, no. 1, pp. 1–12, 2016, doi: 10.1186/s40064-016-1959-1.

[8] M. Nathim, S. Albermany, and Z. M. Hussain, "CRADG: A chaotic RADG security system," *J. Eng. Appl. Sci.*, vol. 12, no. 16, pp. 4118–4122, 2017, doi: 10.3923/jeasci.2017.4118.4122.

[9] S. A. Albermany and G. A. Safdar, "Keyless Security in Wireless Networks," *Wirel. Pers. Commun.*, vol. 79, no. 3, pp. 1713–1731, 2014, doi: 10.1007/s11277-014-1954-1.

[10] Z. Albakaa and S. Albermany, "Improving of RADG Cryptosystem using McEliece and Diffie-Hellman," *Msc thesis, Univ. Kufa, Fac. Comput. Sci. Math.*, no. May 2018, 2018.

[11] A. H. Alwan and S. A. Albermany, "RADG design On Elliptic Curve Cryptography," *ICCIIDT 2016 London - UK Proc.*, vol. 1, pp. 34–46, 2019, doi: 10.1007/978-3-030-05481-6.

[12] J. Bae, C. Hwang, and D. Jun, "The uniform laws of large numbers for the tent map," *Stat. Probab. Lett.*, vol. 80, no. 17–18, pp. 1437–1441, 2010, doi: 10.1016/j.spl.2010.05.010.

[13] X. Wu, B. Zhu, Y. Hu, and Y. Ran, "A Novel Color Image Encryption Scheme Using Rectangular Transform-Enhanced Chaotic Tent Maps," *IEEE Access*, vol. 5, pp. 6429–6436, 2017, doi: 10.1109/ACCESS.2017.2692043.

[14] F. R. Hamade, S. A. K. Albermany, and G. A. Safdar, "New random block cipher algorithm," *Int. Conf. Curr. Res. Comput. Sci. Inf. Technol. ICCIT 2017*, pp. 174–179, 2017, doi: 10.1109/CRCSIT.2017.7965555.