A New Approach of Color Image Encryption Based on RC4 algorithm and Chaotic Map

Dr. Abdul-Wahab Sami Ibrahim
Department of Computer Science
AL-Mustansiriya University
Baghdad, Iraq

Majed Ismael Sameer
Department of Computer Science
AL-Mustansiriya University
Baghdad, Iraq

Abstract: Image Encryption is important for protecting image information, In this paper A chaos based on RC4 algorithm has been proposed to encrypt color Images, It is chaotic Henon function have created three keys , depending on the initial conditions to generate numbers dynamic function of the chaotic conditions in addition to the user's desire three dimensions of which mechanically operated from within the initial condition , and then working process distortion of the bits of the three keys Using the RC4 algorithm and results new in the process of XOR them to generate a unique key of binary bits one and zero and then turn it into a digital fracture and after the intervention to Phase image to encrypted so they generate the keys again, and the size of the desired image In order to encrypt it.

the performance of the algorithm has been analyzed and results show that the algorithm has a very long key space, and high sensitivity for small changes in key which makes the algorithm Immune to Brute force attacks, and it can resist the differential and statistical attacks, in addition to having very high encryption and decryption speed, the receiver can detect any changes to the encrypted image during transmission. the algorithm has been implemented and analysis done by using Matlab R2008a software.

Keywords: Chaos theory, Image Encryption, henon map, symmetrical encryption.

1. INTRODUCTION

Multimedia communications; such as, images, audio and video has become significantly more important, since communications of digital products over the network (wired/wireless) has expanded [1]. There is therefore, Any information shared over Internet needs high level of protection from intruders [2].

The cryptography was used only for the military purposes and diplomatic circles, Cryptography itself divides into two broad categories which are: Asymmetric key algorithms and Symmetric key algorithms [3,4].this paper is used as symmetric key cryptography [5] in which a single secret key is used for both, encryption at sender’s end and decryption at receiver’s end.

Chaotic maps are very complicated nonlinear dynamic systems, which are applied for encryption [6], because they are very sensitive to initial conditions and can generate good pseudorandom sequences.

Chaotic systems have many important properties, such as the sensitive dependence on initial conditions and system parameters.

pseudorandom property, non-periodicity and topological transitivity,[7],Recently, a number of chaos-based encryption schemes have been proposed. Some of them are based on three-dimensional chaotic Henon maps For image encryption. This paper is organized as follows. Section 2, presents an overview on Henon chaotic map system. In section 3 we will discuss the proposed algorithm (RC4 with Chaotic map). Section 4 will present experimental results and analysis. In section 5 we conclude the paper.

2. AN OVERVIEW ON HENON CHAOTIC MAP SYSTEM

In this section, an overview on Henon chaotic map system as important one of the 3-D chaotic map systems, which is used in this work. Henon chaotic map system is described by formula 1 which illustrates a set of the three function of Henon chaotic map system. [8,1]

```
x(i+1)=a-(y(i)^2)-b*(z(i))      |
y(i+1)=x(i)                     |............(1)
 z(i+1)=y(i)                    |
```

when initial values 1.54<|a |<2, 0<|b |<1. and -0.9<=(x or y or z)<=1

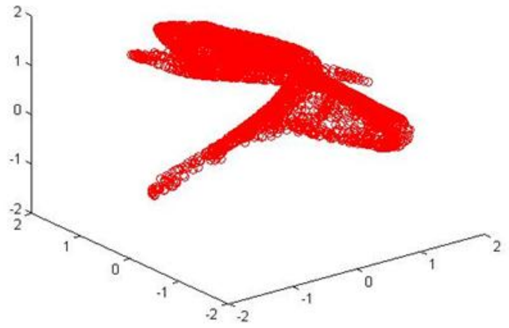
x(1)=1; y(1)=0;z(1)=0; %% Initial conditions The initial value are x=1, y=0.1, z=0,

N=5000; %% let N is the number of iterates example

a=1.6;b=0.2; %% Sets the parameters example

it has a chaotic attractor as shown in Fig.1. It has been experienced that Henon chaotic system is relatively difficult due to the prominent three-dimensional and complex dynamic property[9].

.



Fig(1) three dimension henon map

3. A PROPOSED CHAOTIC MAP AND RC4 ALGORITHM

This paper is dedicated for the designing and implementation of the proposed digital image encryption system. generally, the proposed system encrypts a colored squared digital image using the advantage of chaotic properties to make the encryption more secure and robust against the most known attacks represents the block general diagram for the proposed system in figure(3.2).

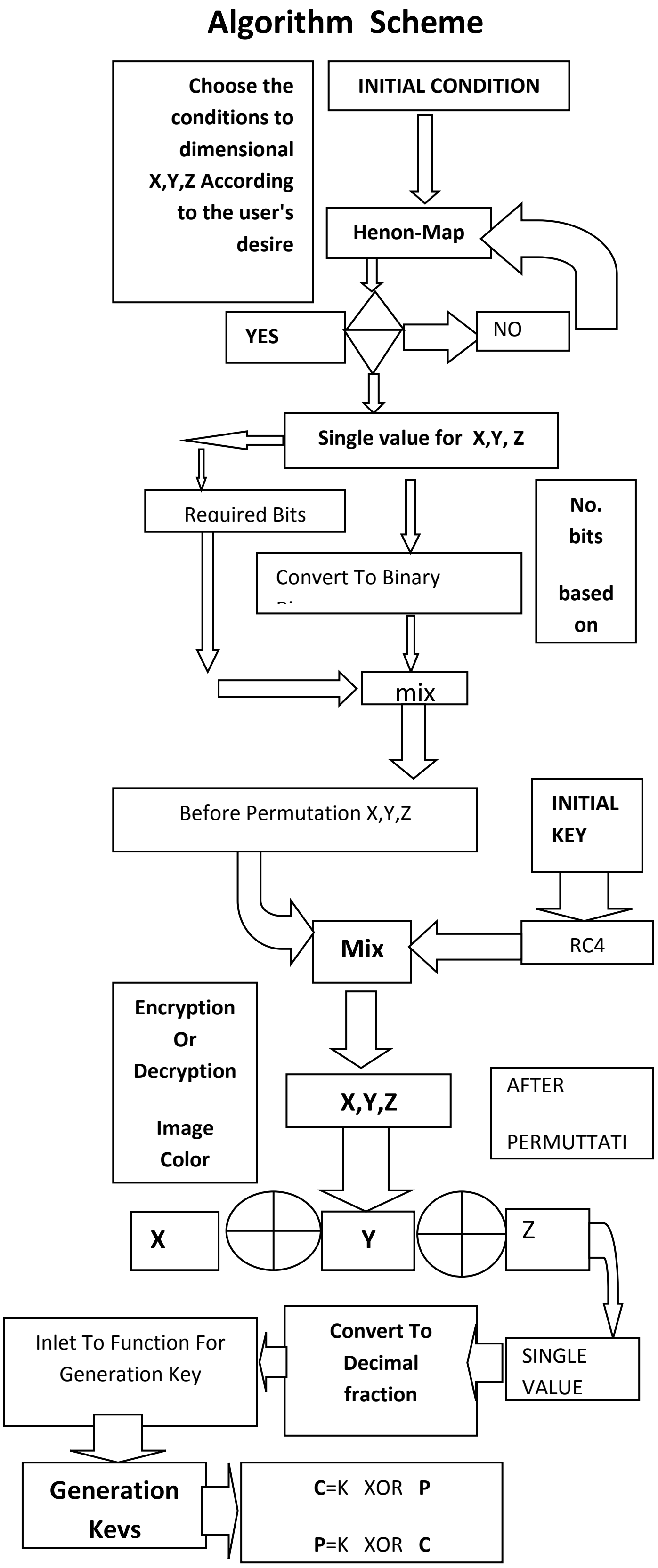


Fig.(3.2) block diagram of the proposed

Chaotic and RC4

The steps for the chaotic and RC4 can be outlined as follows:

Step 1: here used chaotic Henon map three dimension then Select proper initial values and system parameters to create chaotic variable sets .

```
x > -0.9) or x < 1.0 ))
( y> -0.9) or (y < 1.0)
 z > -0.9) or (z < 1.0))
else
'Input out of range!' print ,'Error'
```

Or Desire User's Within This Conditions

Step 2: Prepare the chaotic sequences for range iteration number.

N=number of iteration
  a = 1.4 initial value parameter
  b = 0.3 initial value parameter

step 3: Extracting a single value from step 2
single value for x and single value for y and z
Through the use of condition in step 1 for desire of user condition

step 4: convert results of step 3 to binary
by using function convert decimal fraction to binary

step5: Determine the number of bits specified by the RC4
To create the integer numbers values BY number of bits required BEFORE the PERMUTATION process for X ,Y and Z

step6: Process RC4 Private with permutation is:
part of RC4 algorithm used

```
function [s]=RC41(m) [10]
s=[1:m+1];
T=[1 2 3 7 1 2 3 7 1 2 3 7 1 2 3 7 1 2 3 7 1 2 3 7 1 2 3 7 1 2
3 7 1 2 3 7 1 2 3 7 1 2 3 7 1 2 3 7 1 2 3 7 1 2 3 7];
j=0;
for i=1:m-1 have access.
a=j+s(i+1)+T(i+1);
   j=mod(a,m+1);
   x=s(i+1);
  ; (s(i+1)=s(j+1
 ;  s(j+1)=x
end
end
```

where Initial Permutation = S and T= Initial state

step7: link step4 with step 6 for X,Y and Z
for example 4 bit to step6 is spaced.

Z=t(yy)	Y=v(yy)	X= k(yy))
2	1	2
1	4	3
4	2	1
3	3	4

where yy=1 to 4 but step 4 binary for X,Y and Z

Z	Y	X
0	0	0
1	1	0
0	1	1
1	0	1

then have been obtain

Z	Y	X
1	0	1
0	1	0
1	0	0
0	1	1

step 8:operation XOR between X,Y and Z We obtain with binary bits is XYZ(i) where i number of bits

step 9: convert result for step 8 to decimal fraction By

```
format long
bb=0;
  for i=1:m
     bb=bb+XYZ(i)*2^(-i);
  end
  bb
```

step 10:send result from step9 to function generation key
where bb=result from step 9

```
nn=p*q  ….p=image width q=image height
key = keyGen(bb,nn);
function [key] = keyGen(bb,nn)
n = nn*8;
bi = zeros(n,1,'uint8');
NN= 0;
for m = 1 : n
  NN = 1 - 2* bb* bb;    %based on 1-2*bb^2
    if (NN > 0.0)
       bi(m) = 1;
   end
    bb =  NN;
end
%Intended to produce a binary bits the size of the
%image *8……..>>>bi
key = zeros(n/8,1,'uint8'); %Reset keys
for k = 1 : n/8
   for j = 1 : 8 % here reason to use 8
   key(k) = key(k) + bi(j*k)* 2 ^ (j-1); %based on levels color
2^8
 end
end
```

here generated keys by size nn=p*q ….p=image width q=image height

step 11: stage encryption

When we got the keys to the image size from step 10 for p*q then we will encryption image and so based on Operation XOR for keys from step 10 with each component of the three color components red ,green and blue Based on these relations Confusion

step 12:stage decryption

take the image encryption based on the same key for plain image with XOR operation to obtain plain image.

4. EXPERIMENTAL RESULTS AND ANALYSIS

In this paper , a practical programs of a proposed algorithm and a practical programs of all experimental and security analysis tests are designed by using MATLAB language release R2008a for 64bit Windows 7 Home Premium operating system. The computer used to perform these tests is a Dell Laptop with Intel (R) Core™ i3-3217u CPU@ 1.8GHz and 6 GB installed memory.

4.1 Statistical Analysis

4.1.1 Histogram Analysis

Histogram analysis of three channels (red, green, and blue) of the plain and encrypted images is given. Figure (4.1.1) shows the histograms of the 512*512 plain and encrypted. It is observed that the histograms of the encrypted image are significantly different from that of the plain image(lena.png).

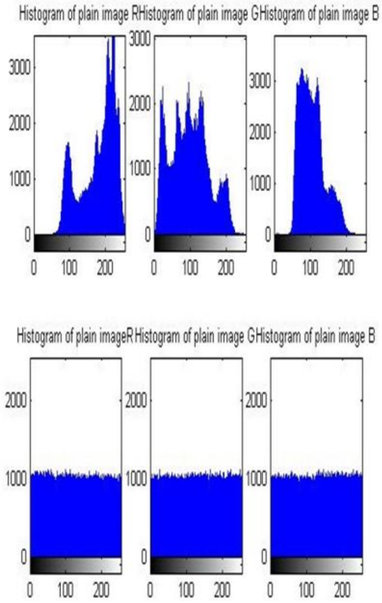
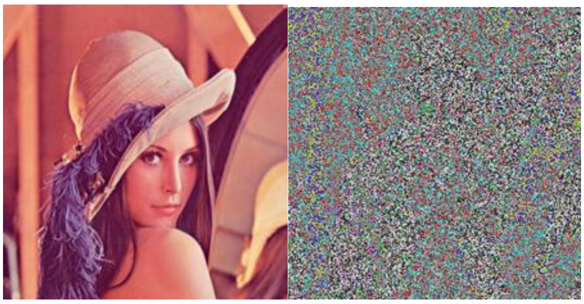


Figure (4.1.1) shows the histograms of the 512 × 512 plain and encrypted.

4.1.2 Correlation coefficient Analysis

In this section the horizontal, vertical and diagonal correlation coefficient of the pixels studied. To do this we choose 2048 pairs of horizontal, vertical and diagonal adjacent pixels randomly. Figure (4.1.2) show the distribution of two horizontally, vertically and diagonally adjacent pixels in plain image and encrypted image[11]



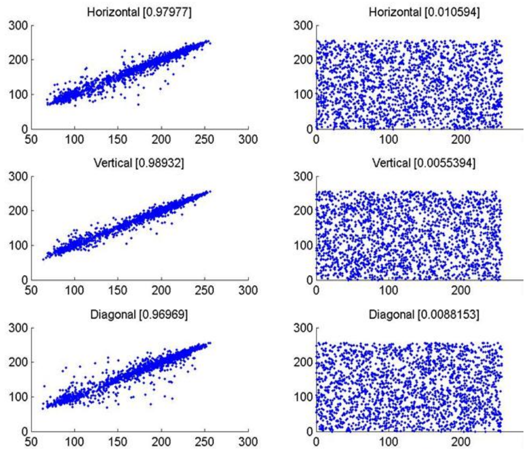


Figure (4.1.2) Correlations of two diagonal, horizontally and vertical adjacent pixels in the plain image and in the cipher-image

The correlation coefficient of two adjacent pixels calculated using in[12,11] formula 2

$$E(x)=\frac{1}{N}\sum_{i=1}^{N} xi$$

$$D(x)=\frac{1}{N}\sum_{i=1}^{N}(xi-E(xi))$$

$$cov(x,y)=\frac{1}{N}\sum_{i=1}^{N}\big(xi-E(xi)\big)\big(yi-E(yi)\big)......(2)$$

$$Rxy=\frac{cov(x,y)}{\sqrt{D(x)}\sqrt{D(y)}}$$

where x and y are the value of two adjacent pixels in the image and N is the total number of pixels selected from the image for the calculation[21] ,following results for found for various standard images in table(1).

Table (1) Correlation coefficient of two adjacent pixels in plain image and encrypted image for 'lena.png' 256*256*3 size image

state	Plane image	Encrypted image
Horizontal	0.9798	0.0106
Vertical	0.9893	0.0055
Diagonal	0.9697	0.0088

In Table (1) have been obtain the correlation coefficient for the plain and encrypted images shown in figure 4.1.2(a,b,c) , It is clear from the Table (1) that there is negligible correlation between the two adjacent pixels in the encrypted image . However, the two adjacent pixels in the plain image are highly correlated.[11]

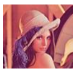
4.1.3 The Information Entropy Analysis

Entropy is a measure of uncertainty association with random variable. As for an image, the encryption decreases the mutual information among pixel values and thus increases the entropy value. A secure system should satisfy a condition on the information entropy that is the cipher image should not provide any information about the original image.[13]. It is defined as follows in formula 3:

$$\mathbf{H (X) = -\sum_{i=0}^{255} p (X i) \log 2 \, p (X i)} \; \mathbf{…………(3)} \quad ,$$

where X is a discrete random variable, p(x) is the probability density function of the occurrence of the symbol x .Its value for gray scale encrypted image should be very close to ideal value 8. Information entropy analysis is applied on the standard test images and their encrypted images. The results are listed in the Table (2). The values listed in the Table (2) are the average value for the three color bands for the plain images and the encrypted images.

According to the results shown in Table (2) , the proposed system achieved a high permutation and substitution, and it is strong enough against the Entropy Attack because the information entropy value for the encrypted images are very close to the idealism value mentioned above.[14] Table(2)The Information Entropy for the Plain and Encrypted Image

Plain image	Entropy for plain image	Entropy for Encryption image
	6.6638	7.9920
	7.7502	7.9918

4.2 Security Differential Attack Analysis

One minor change in the plain image causes large changes in the cipher image then differential analysis may become useless thus, much difference between encrypted forms is expected in order to keep high security[15] It is a common measure used to check the effect of one pixel change on the entire image. this will indicate the percentage of different pixels between two images[16]Often the attacker slight change such as changing the value of a pixel one point in the image the encrypted using the algorithm and concludes the relationship between the two pictures encryption image before and after the change, this is called chosen plaintext attack (differential attack) attack to find a certain relationship between the encrypted image and the original image to infer the secret key according to this differential attacks do not be successful relationship, If a major change is the work the following differential analysis to measure the efficiency of the algorithm against differential attacks[17,18] so that used : NPCR and UACI

NPCR measures the percentage of different pixels numbers between two cipher-images whose plain images only have one-pixel difference. UACI measures the average intensity of differences between two cipher images. to resist difference attacks, the values of NPCR and UACI should be large enough Value has changed one bit of image Baboon The calculated ratios before and after change And bring the same accounts after changing the value of a pixel one point or 8 bits, and the results obtained were within the specified percentages Ideal for encryption in[19].Table(3)show the results obtained.

Table(3)values of NPCR and UACI at change pixel I(250,250,2) FROM 147 TO 2

compound color	NPCR	UACI
R	99.5841979980469	33.2961452708525
G	98.6638011	32.9332814
B	99.6021270751953	33.2787173402076
TOTAL	99.6093750000000	33.4635416666667

4.2.1 Key space analysis

The used key must not be long or short . short key can be easily obtained when applying brute -force attack or analysis . security encryption system that is dependent on the key according to the laws Kirchhoff As long key reduces the speed of system performance This is undesirable because the encryption of important specifications for the design speed of the encryption system. Must not be less than the key space 2^100, to provide a high level of safety. In the proposed algorithm has been used chaotic Henon function maps were generated keys, and each requires a series initial value and control value for chaotic map. where they are used as keys for encryption, if the primary control variables and values accurately in 10^14, the total area of the key

10^14*10^14*10^14*10^14*10^14=10^70=2^232 that length 232 bit very good for resistant brute attack.

In addition to the keys to the sensitivity of algorithm RC4 FOR X,Y,Z

for example in X DIMENSION

T=[1 2 3 7 1 2 3 7 1 2 3 7 1 2 3 7 1 2 3 7 1 2 3 7 1 2 3 7 1 2 3 7 1 2 3 7 1 2 3 7 1 2 3 7 1 2 3 7 1 2 3 7 1 2 3 7 1 2 3 7];

in RC4 ,and also

Y DIMENSION

T=[5 2 3 6 5 2 3 6 5 2 3 6 5 2 3 6 5 2 3 6 5 2 3 6 5 2 3 6 5 2 3 6 5 2 3 6 5 2 3 6 5 2 3 6 5 2 3 6 5 2 3 6 5 2 3 6 5 2 3 6];

and also

Z DIMENSION

T=[1 2 5 6 1 2 5 6 1 2 5 6 1 2 5 6 1 2 5 6 1 2 5 6 1 2 5 6 1 2 5 6 1 2 5 6 1 2 5 6 1 2 5 6 1 2 5 6 1 2 5 6 1 2 5 6 1 2 5 6];

Any change in the value of values the keys will be sensitive to those changes decryption when change any value key in case of attack. then the total area of the keys

10^14*10^14*10^14*10^14*10^14*10^14*10^14*10^14=10 ^112=2^372

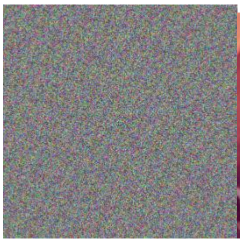
These keys are the very least it is possible to the increment depend on user's desire. As well as sensitivity to the number of iterations and the number of bits required for all anti-brute force attacks.

4.2.2 Key sensitivity analysis

In addition to being long enough to give the key safety system, the ideal encryption system must be very sensitive to any A slight change in the secret key , and any slight change in the used key must lead to the generation of an entirely different encrypted image before the change in the key image encrypted, and this ensures that the system resistant to brute force attack, done several experiments to test Over the system's sensitivity to a change in the key as follows[20]:

1. initial value use as X as a key to generate a first series of numbers chaotic , It was obtained on image encryption fig(4.2.2.b)from plain image (4.2.2. a)

2. use the same key with a few difference by X+10^(−13) as an experiment to decode the encrypted to image encryption, but we got another encrypted image to fig(4.2.2. c). This shows how the algorithm immunity against brute force attacks as the slight change in the key 1* 10^{-14} To extract the original image failure.

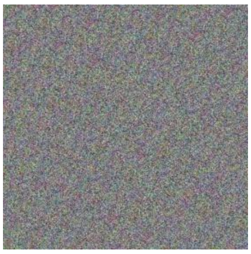


plain image

FIG(4.2.2.a)

encryption image by use key X

FIG(4.2.2. b)



Fig(4.2.2.c)image extract after using the wrong key By Differentiate a little by .00000000000001 for the correct key the same processes as possible having to RC4 for X or Y or Z DIMENSIONS.

4.3 Performance analysis

Encryption of the important requirements of the system performance of the system speed after a safety investigation, the table (4) Includes average time it takes Windows 7 environment within Matlab R2008a to encrypt and decrypt images standard listed in the table using a program 6GB RAM processor 1.8 Ghz and Intel core quickly on a personal calculator has the following specifications in table (4)

Image and size 512*512*3	Time of encrypted	Time of decode the encrypted
Lenna.png	13	4
Baboon.png 512*512*3	12	4
Airplane.png 512*512*3	11	4

table(4) The average time taken to implement encryption

5. Conclusions

It has been proposed algorithm to encrypt the image of color, Using chaotic theory with part of the algorithm RC4. Henon function used of three dimensions of the function chaotic, The encryption and decryption process images very successful so that and by work of procedure the statistical analyzes and differential, And measuring and analyzing the efficiency of encryption key length and its sensitivity to change and measure the speed of implementation of the algorithm. the results showed robustness against the attacks statistical, the sensitivity is sufficient to change the secret keys for resist generally brute force . as well as the results proved to possess the speed of implementation of the algorithm high of close to real time. While providing a mechanism if it's been encrypted during transfer to a change in the values of image points, or manipulated by knowing NPCR and UACI

*6.*REFERENCES

[1] Alia Karim Abdul Hassan," Proposed Hyper chaotic System for Image Encryption"*(IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 7, No. 1, 2016.*

[2] N. S. RAGHAVA & ASHISH KUMAR," IMAGE ENCRYPTION USING HENON CHAOTIC MAP WITH BYTE SEQUENCE", International Journal of Computer Science Engineering and Information Technology Research (IJCSEITR) ISSN(P): 2249-6831; ISSN(E): 2249-7943 Vol. 3, Issue 5, Dec 2013, 11-18.

[3] *.B. A.Forouzan, "Cryptography and Network Security", Mc Graw Hill, International Edition, 2008*

[4] *B. Schneier and N. Fergusson,"Practical Cryptography", Wiley Publishing, Inc., First Edition, 2003.*

[5] *W. Stallings,"Cryptography and Network Security Principles and Practice", Fifth Edition, Pearson Education, Prentice Hall publishing, 2011.*

[6] Osama M.Abu Zaid, Moussa Demba, Mohamed A.AL-Refaiy," Confusion Algorithm based on 3-D Chaotic Map System for Securing the Colored Images *"International Journal of Computer Applications (0975 – 8887) Volume 72– No.10, June 2013*

[7] Zhang LH, Liao XF, Wang XB. An image encryption approach based on chaotic maps. Chaos, Solitons & Fractals, Vol. 24, pp. 759–765., 2005
8. Pianhui Wu , Weihua Zhao b, Zhengxu Zhao c," Hyper chaotic Based-on Henon Map",Journal of Information & Computational Science 11:12 (2014)

[9] S. V. GONCHENKO Inst. Appl. Math. and Cyb., Nizhny Novgorod State Univ., 10 Ulyanova st., Nizhny Novgorod, 603005, Russia gosv100@uic.nnov.ru,"THREE-DIMENSIONAL H´ENON-LIKE MAPS AND WILD LORENZ-LIKE ATTRACTORS", Received October 15, 2004; Revised February 15, 2005, International Journal of Bifurcation and Chaos, Vol. 15, No. 11 (2005) 3493–3508

[10] Ricardo Goulart, " Considerações sobre o algorithm RC4.", Universidad Federal do Rio Grande do Sul PGCC - Pós-graduação em Computação,2000

[11] Kamal Jadidy Aval, Morteza Sabery Kamarposhty, Masumeh Damrudi," A Simple Method for Image Encryption Using Chaotic Logistic Map *"Journal of Computer Science & Computational Mathematics, Volume 3, Issue 3,September 2013.*

[12] Mintu Philip," AN ENHANCED CHAOTIC IMAGE ENCRYPTION" International Journal of Computer Science, Engineering and Information Technology (IJCSEIT), Vol.1, No.5, December 2011

[13] Rakesh S, Ajitkumar A Kaller, Shadakshari B C and Annappa B*,"* Multilevel Image Encryption*",* Department of Computer Science and Engineering, National Institute of Technology Karnataka, Surathka ,2003

[14] Mustafa A. Hussain AL-Nuaimi , " Color Image Encryption Based on Chaotic Maps", *Submitted to the College of Science / Al-Mustansiriyah University,1999*

[15] Narendra K Pareek," DESIGN AND ANALYSIS OF A NOVEL DIGITAL IMAGE ENCRYPTION SCHEME",International Journal of Network Security & Its Applications (IJNSA), Vol.4, No.2, March 2012

[16] Amber Shaukat Nasim," CHAOS BASED CRYPTOGRPHY AND IMAGE ENCRYPTION", M.Sc., University of Applied Sciences, Luebeck, Germany, 2012

[17] Fakhrulddin H. Ali*,*Maha Basher Hussein*,"* Colored Image Encryption Algorithm Using DNA Code and Chaos Theory*",* Second Engineering Conference, the Golden Jubilee of the College of Engineering - University of Mosul,2013

[18] Dr.S.Ramahrishnan1,B.Elakkiya2R.Geetha3,P.Vasuki4, 1Professor & head, 2, 3, 4 UG Scholars," Image Encryption Using Chaotic Maps in Hybrid Domain" International Journal of Communication and Computer Technologies Volume 02 – No.13 Issue: 05 June 2014 ISSN NUMBER : 2278-9723

[19] Yue Wu, Joseph P. Noonan, Sos Agaian," NPCR and UACI Randomness Tests for Image Encryption",Cyber Journals: Multidisciplinary Journals in Science and Technology, Journal of Selected Areas in Telecommunications (JSAT), April Edition, 2011

[20] Narendra K Pareek," DESIGN AND ANALYSIS OF A NOVEL DIGITAL IMAGE ENCRYPTION SCHEME", International Journal of Network Security & Its Applications (IJNSA), Vol.4, No.2, March 2012.

[21] Narendra K Pareek, Vinod Patidar, K.K. Sud," Image encryption using chaotic logistic map",publication at:https://www.researchgate.net/publication/215658784,January 2006