Vol. 1 No.1, July 2021

FUAM Journal of Pure and Applied Science

Available online at
www.fuamjpas.org.ng

An official Publication of
College of Science
Joseph Sarwuan Tarka University,
Makurdi.

FUAMJPAS

FUAM Journal of Pure and Applied Science

© College of Science, Joseph Sarwuan Tarka University, Makurdi

https://fuamjpas.org.ng/

Vol.1. No. 1. July, 2021

Digital Image Encryption and Decryption

[1*]T. Gbaden and [2]A.R. Gbaden

[1]Department of Mathematics/Statistics/Computer Science, Joseph Sarwuan Tarka University, Makurdi, Benue State, Nigeria

[2] Department of Mathematics/Computer Science, University of Mkar, Mkar Gboko, Benue State, Nigeria

***Correspondence E-mails**: gbaden2014@gmail.com ; wanvadoo@gmail.com

Received: 19/04/2021 Accepted: 24/07/2021 Published online: 10/08/2021

Abstract

As we live and revel in a digital age, the day to day transmission of multimedia data over the internet is beyond our imaginations. Consequently, the increased risk of losing or altering the data during transit is more. Protection of this multimedia data (audio/speech, image and video) becomes one of the major security concerns, because millions of internet users worldwide are infringing digital rights daily, by downloading multimedia contents illegally from the internet. The image protection is very important, as the image transmission covers the highest percentage of the multimedia data. Image encryption is one of the ways out to achieve this. Our world built upon the concept of progression and advancement, has entered a new scientific realm known as chaotic theory. Chaotic encryption is one of the best alternative ways to ensure security. Many image encryption schemes using chaotic maps have been proposed, because of its extreme sensitivity to initial conditions, unpredictability and random like behaviours. Each of them has its own strengths and weaknesses. In this work, we propose a chaotic data encryption method based one dimensional exponential chaotic map. We used the chaotic cryptographic models to encrypt standard images stored in tif format. The experimental result demonstrates that the proposed algorithm can be used successfully to encrypt/decrypt the images with the secret keys.

Keywords: Encryption, Logistic map, Chaos, Cryptography

Introduction

Digital information in the form of images and other multimedia files are frequently transmitted via computer networks across untrusted networks. This is prone to security threats since continuous attempts are made by hackers to alter or illegally own such information during communication that might profit them without the awareness of the appropriate receiver [1];[2]. Such alterations can cause a major disaster since reliable transmission of images, is needed in many applications such as military operations, business transactions and medical systems [3]. In the light of the foregoing, there is need to protect image information from unauthorized access, guarantee their content from the change and prevent them from network attacks during transmission [4].

In this work, improved image encryption algorithm based on one dimensional exponential logistic chaotic map is addressed, with the goal of providing an efficient and secure way for image encryption. Due to extensive information within a digital image, divulged image contents sometimes cause severe problems for its owners [5]. In many cases, such information leakage seriously invades personal privacy, example, the malicious spread of photos in personal online albums or patients medical diagnosis images and furthermore, it may cause uncountable losses for a company or a nation. For example, secret products design for a company or a governmental classified scanned document. Traditional encryption systems like Digital Encryption Standard (DES), Advanced Encryption Standard (AES), International Data Encryption Algorithm (IDEA), Rivest_Shamir_Adleman (RSA) are not well suited for image encryption. Because in these encryption schemes there exist high correlation among pixels, so it takes high computation time and power [6].

Related works

The fast-growing demand of transmitting images via public networks has raised interest in chaos. Chaos is an interesting phenomenon that often happens in many physical systems [7]. Properties of chaos, such as randomness and ergodicity, have proved to be suitable for designing the means for data protection. During the past decade, many chaos-based cryptographic techniques have been studied, such as the chaos-based secret communication, chaos-based block/stream cipher and chaos-based random number generation [8]. Additionally, some applications based on chaos have been investigated. For example, chaos-based image encryption or authentication, video/audio scrambling, multimedia and copyright protection. Chaos-based cryptography is a research field across two fields, i.e., chaos (nonlinear dynamic system) and cryptography (computer and data security) [9].

Chaotic maps are very suitable for constructing encryption algorithms, their high sensitivity to initial values and parameters makes the algorithms to be effective and robust. In addition, chaotic ciphers are generally easy to implement and have fast speed, low resource consumption, which shows a clear advantage for multimedia data encryption. Therefore, chaotic maps provide a good application for the secure transmission of multimedia data encryption [10]; [11].
In this work, improved image encryption algorithms based on chaotic maps are developed, with the goal of providing an efficient and secure way for image encryption.

The one-dimensional logistic map

One of the most studied examples of a one-dimensional system capable of various dynamical regimes including chaos is the 1-D logistic map. It is a representation of an idealized population growth model and is defined by the equation

$$x_{n+1} = f(x_n) = rx_n(1 - x_n) \qquad (1)$$

where $x_n \in [0,1]$ and represents the population at year *n*, and hence x_0 represents the initial population at year 0. Crucial to the behaviour of the map is the control parameter $r \in [0,4]$ whose dynamical behaviour is very complicated and it represents a combined rate for reproduction and starvation. Slight changes in the parameter, "*r*", of the map can cause the iterated map to change from stable and predictable behaviour to unpredictable behaviour which is called chaos. We begin the analysis of the logistic map by finding its periodic points and observe how orbits qualitatively change as the control parameter *r* is varied. This helps in illustrating the concepts of bifurcations and chaotic motions. To find the fixed points of the map (also called points of period one), it is necessary to solve the equation given by$f(x) = rx(1 - x) = x$ which gives the points that satisfy the condition$x_{n+1} = x_n$for all n. Two solutions were found: $x_{1,1} = 0$ and $x_{1,2} = 1 - \frac{1}{r}$.

Weaknesses of the one-dimensional logistic map

The one dimensional chaotic system's drawbacks include small key space and weak security. Logistic maps are faced with the problem of lack of robustness of their encryptions because of round off errors in real number quantization. This may lead to nonreversible functions for encryption and this makes decryption process impossible. The third defect reveals a high risk that initial values and parameters used in a chaotic system might be fully analyzed using existing tools and methods after a long term observation.

The One-Dimensional Exponential Logistic Map

The proposed one dimensional exponential logistic map is defined by

$$x_{n+1} = f(x_n) = rx_n(1 - x_n)e^{x_n}, \qquad (2)$$

where $x_n \in [0,1]$ and where $r \in [0\ , 2.25]$ is the control parameter. Slight changes in the values of the parameter, "r", of the map can cause the iterated map to change from stable and predictable behaviour to unpredictable behaviour which is called chaos. Equation (2) is an improved model of (1) developed by May and Feigenbaun which became a paradigm of chaotic bahaviour in the 1970s [8]. The exponential function e^{x_n} provides complexity then improved security to the encrypted image.

Image encryption algorithm using the exponential logistic map

In this section, we present the detail algorithm for encryption/decryption of gray scale images using modified 1-D logistic map.

Encryption algorithm

i. Read the original image I.
ii. Obtained the image dimension as axbx3 for RGB images or axb for gray scale images.
iii. Compute the number of pixels in I as N= axbx3 (RGB) or a x b (Grayscale).
iv. Read the parameters value for the x_1 and r.
v. Evaluate the logistic map up to N-1 times to generate vector X.
vi. Add confusion to the vector X with mod function.
vii. Convert the vector X to uint 8.
viii. Perform the encryption using bit XOR operation.

ix. Save the encrypted image in the file named I2.
x. Display the encrypted image from file I2.

Decryption algorithm

i. Read the encrypted image file I2.
ii. Obtain the image dimension as a x b x 3.
iii. Compute number of pixels in I2 as N=axbx3.
iv. Enter your parameters value for y_1 and r.
v. Evaluate the logistic map up to N-1 times to generate vector Y.
vi. Confuse the vector Y with mod function.
vii. Convert vector Y to uint8.
viii. Perform the decryption process using bit XOR operation.
ix. Save the decrypted image as I3.
x. Display the decrypted image I3.

Flowchart diagram for the encryption/decryption using the exponential logistic map

Encryption

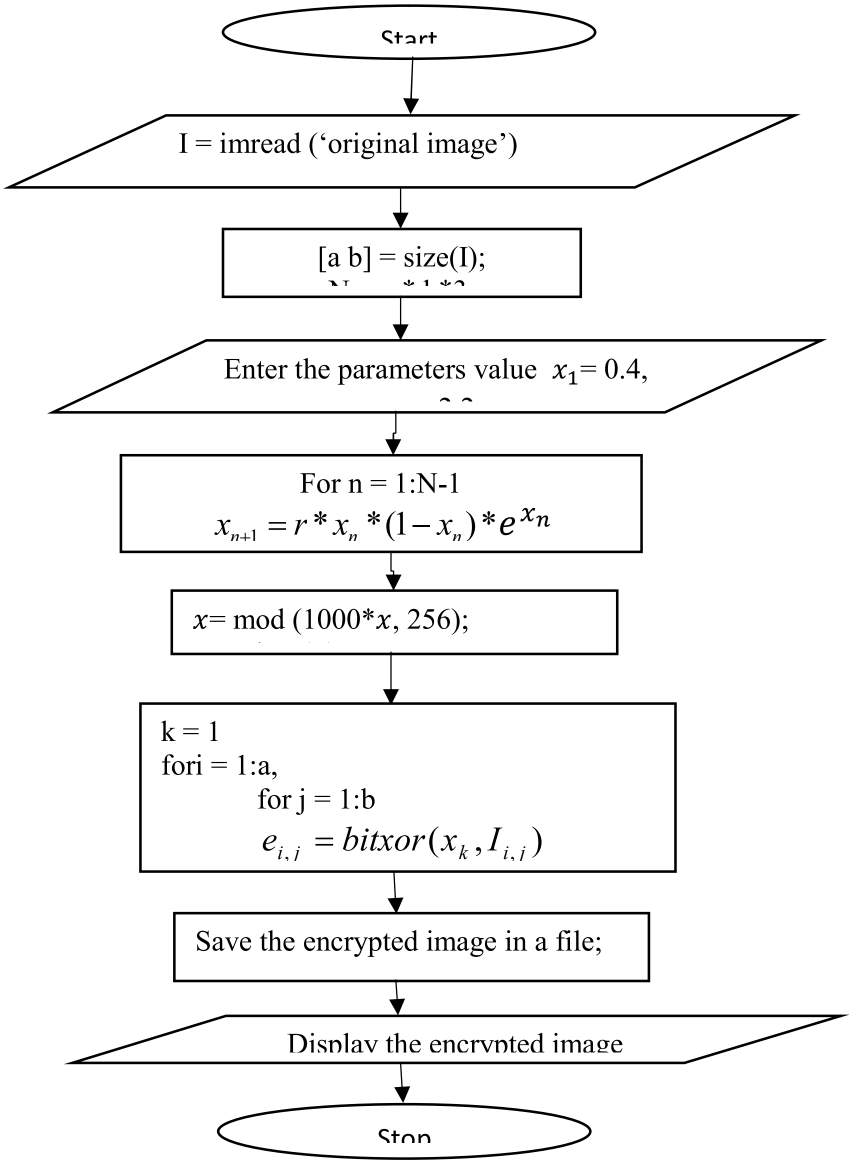

Start
I = imread ('original image')
[a b] = size(I);
Enter the parameters value x_1= 0.4,
For n = 1:N-1
$x_{n+1} = r * x_n * (1 - x_n) * e^{x_n}$
x= mod (1000*x, 256);
k = 1
fori = 1:a,
for j = 1:b
$e_{i,j} = bitxor(x_k, I_{i,j})$
Save the encrypted image in a file;
Display the encrypted image
Stop

Figure 1: Flowchart diagram for the encryption using modified 1-D logistic map.

Decryption

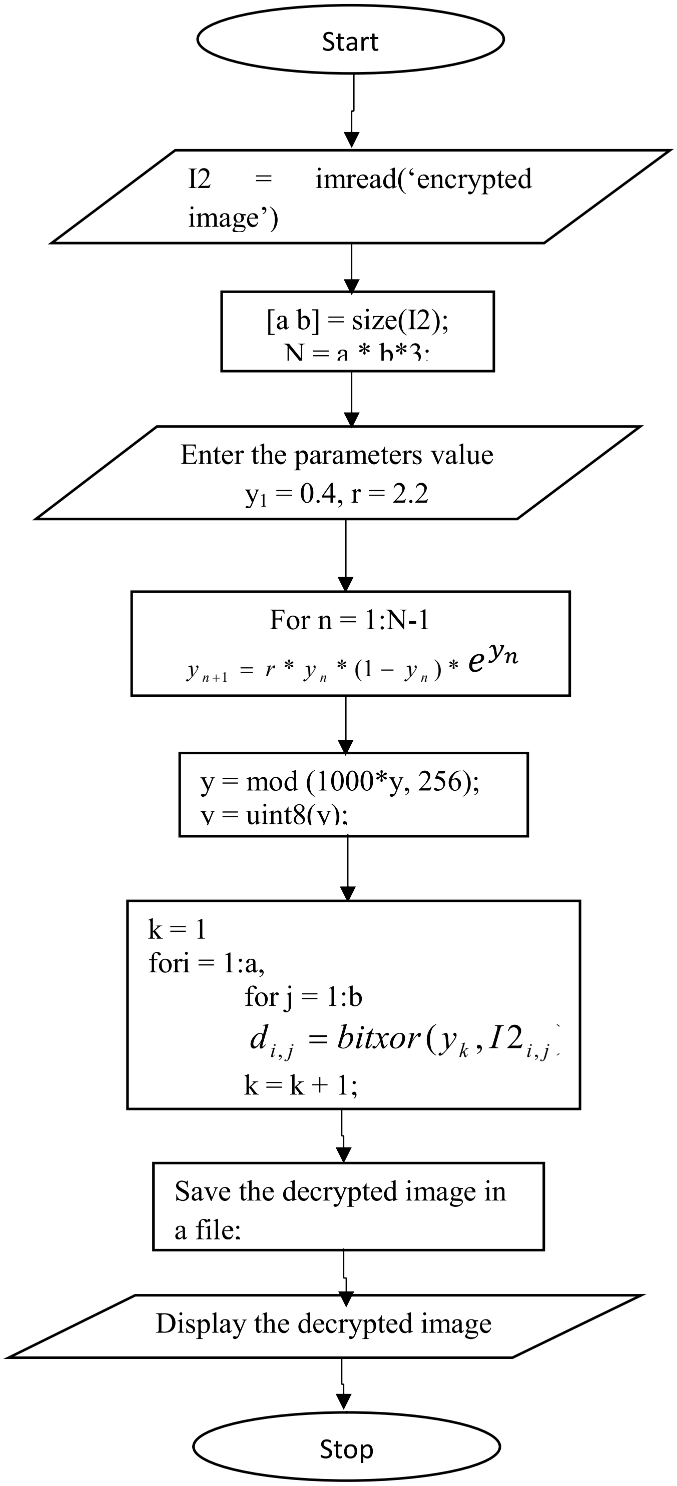

Start
I2 = imread('encrypted image')
[a b] = size(I2);
N = a * b*3;
Enter the parameters value
$y_1 = 0.4$, r = 2.2
For n = 1:N-1
$y_{n+1} = r * y_n * (1 - y_n) * e^{y_n}$
y = mod (1000*y, 256);
y = uint8(y);
k = 1
fori = 1:a,
for j = 1:b
$d_{i,j} = bitxor(y_k, I2_{i,j})$
k = k + 1;
Save the decrypted image in a file:
Display the decrypted image
Stop

Figure 2: Flowchart diagram for decryption using modified 1-D logistic map.

Results and Discussion

Hardware Requirement for the Implementation

Processor: a minimum of 500 MHZ Pentium processor is required. It is however recommended that for optimum performance faster processors like 1.5 GHZ Pentium grade processor or higher can be used.

RAM size: the minimum RAM requirement is 512 MB but 4GB is recommended for flawless execution.

Disk Space: a minimum of 20 GB of hard disk space is required. The user may be able to make more space available by removing temporary files on the computer.

Software Requirement for the Implementation

The software requirements include a minimum of the following:
Microsoft Windows XP Home and Professional edition.
Coding Language Jdk 12.0.2
IDE- Net Beans 8.1

The properties of one-dimensional exponential logistic map

The one-dimensional exponential logistic map is a simple non linear model, but it has complicated dynamical behaviour. The chaotic sequence produced by the logistic map is extremely sensitive to the change of its initial value. The sequences produced by the map are controlled by parameter value "r" and initial value x_0. The system has different characteristics with different values of r, called bifurcation parameter. The proposed one dimensional exponential logistic map is defined by (3.4) where $x_n \in [0,1]$ and $r \in [0\,,2.25]$ is the control parameter. Slight changes in the values of the parameter, "r", of the map can cause the iterated map to change from stable and predictable behaviour to unpredictable behaviour which is called chaos. Figure 2 shows the bifurcation diagram of the exponential logistic map. From the figure we observed that when the control parameter *r*< 1, all the points are plotted at zero, i.e. zero is the one-point attractor for *r*< 1. The figure also shows that when 1 <*r*<1.8, we still have a one point attractors, but the "attracted" value of x increases as *r* increases, at least to 1.8. Bifurcations occur first at *r* = 1.8, then *r* = 1.97 and *r* = 2.02 (approximately) until just beyond *r* = 2.15 where the system becomes chaotic up to *r* = 2.25 which can generate a chaotic sequence in the region (0,1). The orbits escape to infinity for *r*> 2.25.

Plotting of the maps

The following graphs shows:
(i) Periodicity when 0<r<2, $x \in (0,1)$ $x_0 = 0.6$.
(ii) Chaos when 2<r<2.25, $x \in (0,1)$ $x_0 = 0.6$,
(iii) Escape to infinity when r>2.25, $x \in (0,1)$ $x_0 = 0.6$.

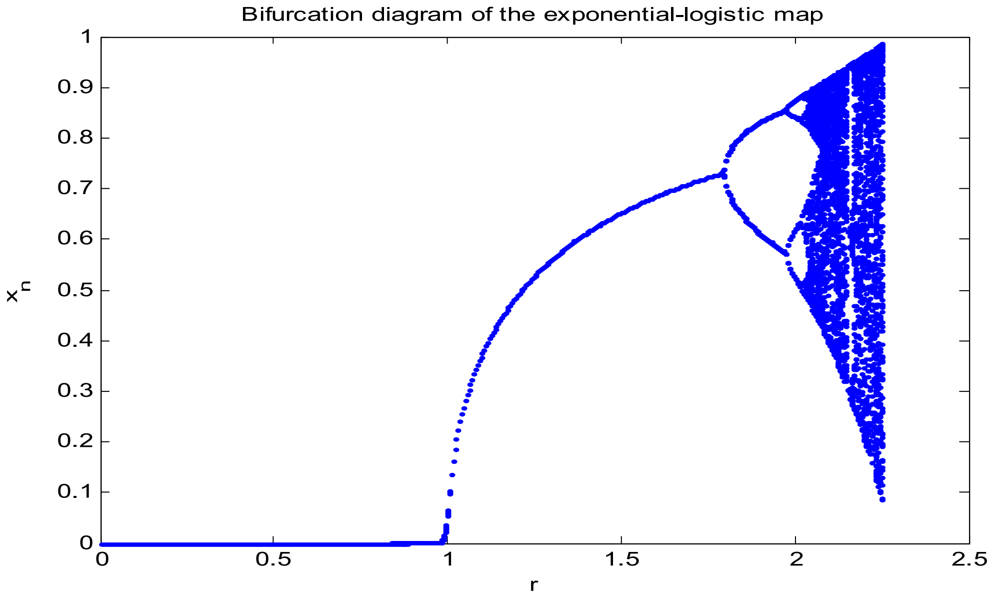


Figure 3: Bifurcation Diagram of the Exponential Logistic Map

Figure 3 shows the bifurcation diagram of the exponential logistic map which shows the region of (i) Periodicity when 0<r<2, $x \in (0,1)$ $x_0 = 0.6$,

(ii) Chaos when 2<r<2.25, $x \in (0,1)$ $x_0 = 0.6$,

(iii) Escape to infinity when r>2.25, $x \in (0,1)$ $x_0 = 0.6$. The illustration above shows a bifurcation diagram of the exponential logistic map obtained by plotting as a function of r a series of values for x_n obtained by starting with a random value x_0, iterating many times, and discarding the first points corresponding to values before the iterates converge to the attractor.

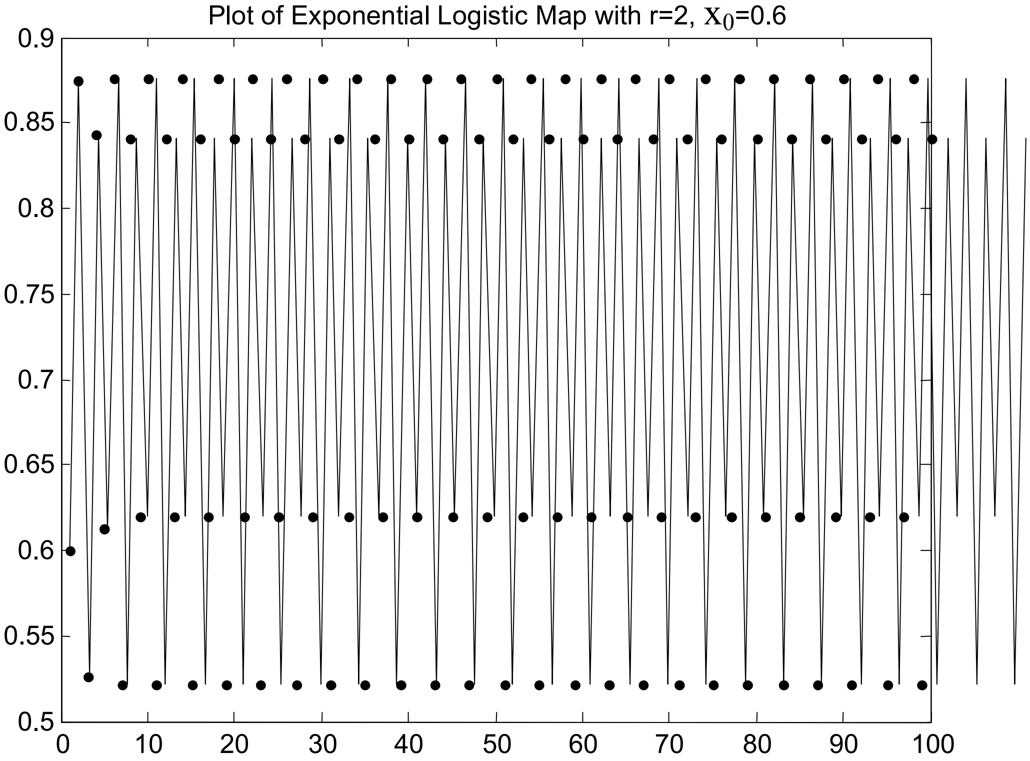


Figure 4: Plot of Exponential Logistic Map showing Periodicity

Figure 4 shows periodicity of the exponential logistic map. There is regularity in the plots displayed.

Figure 5 displays the irregularity otherwise known as chaos of the exponential logistic map. Here lies the point of interest of the research as it becomes very difficult to predict the behavior of the encryption even after a careful study of the map.

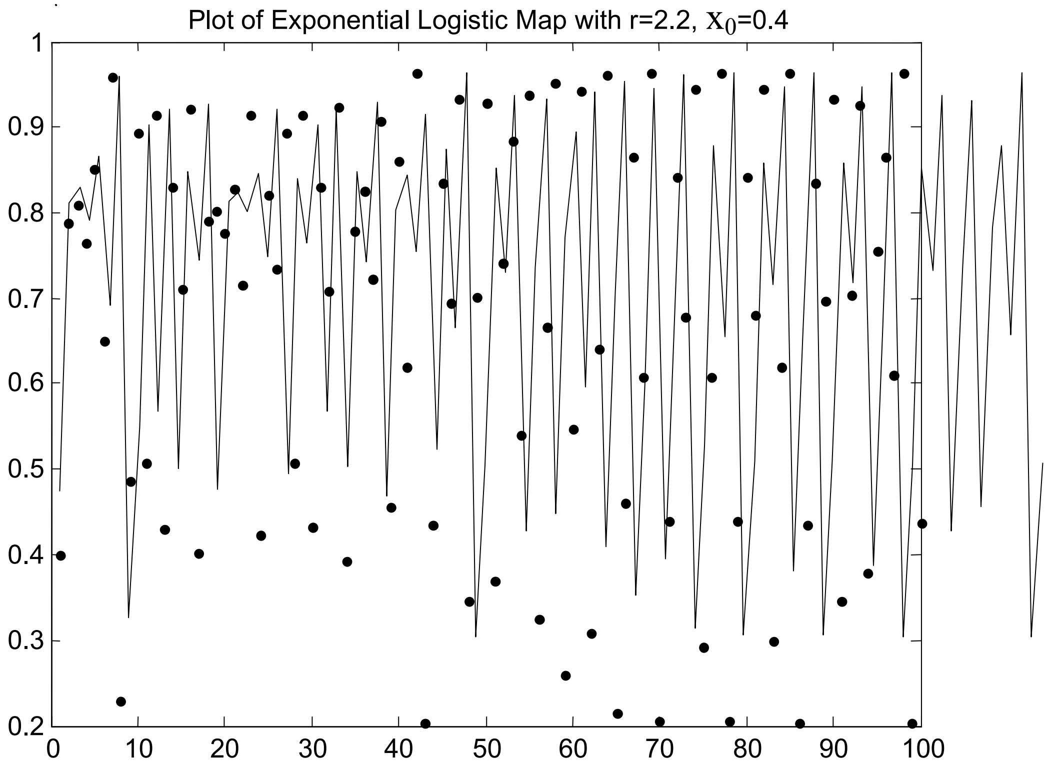


Figure 5: Plot of Exponential Logistic Map showing Chaos

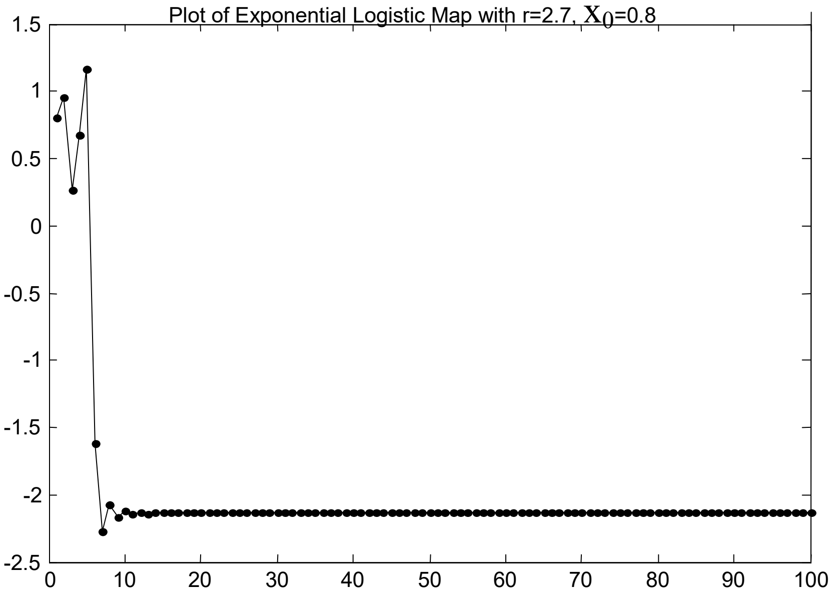


Figure 6: Plot of Exponential Logistic Map showing Escape to Infinity

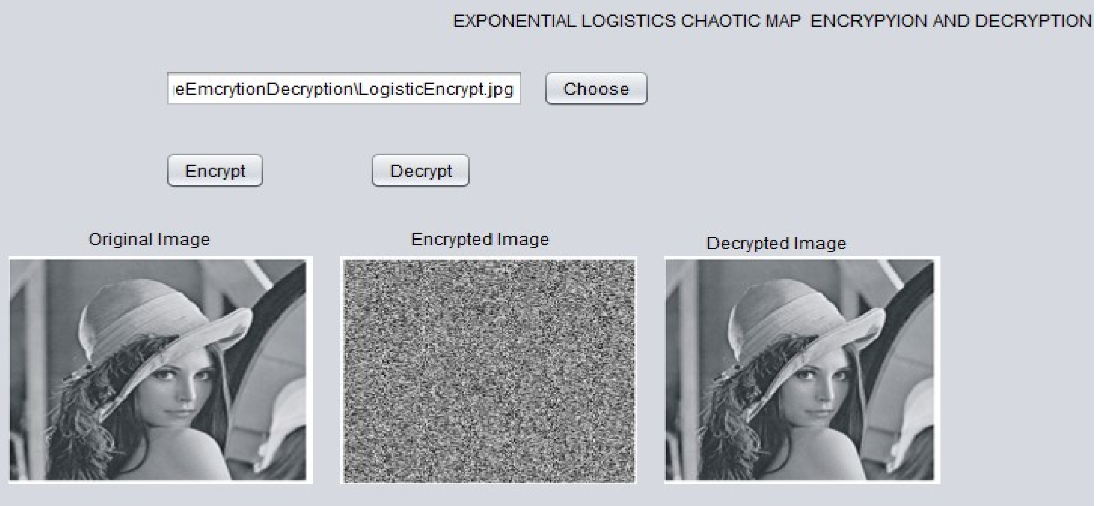
Figure 6 shows escape to infinity. The map can no longer be under control.

Experimental results

We conducted this experiment using hp 250 G5 computer with a processing speed of 1.6GHz and a RAM of 2048MB.

Three images were used to test the proposed one-dimensional exponential logistic encryption algorithm; lena_gray_256.tif, peppers_gray_256.tif. and mandril

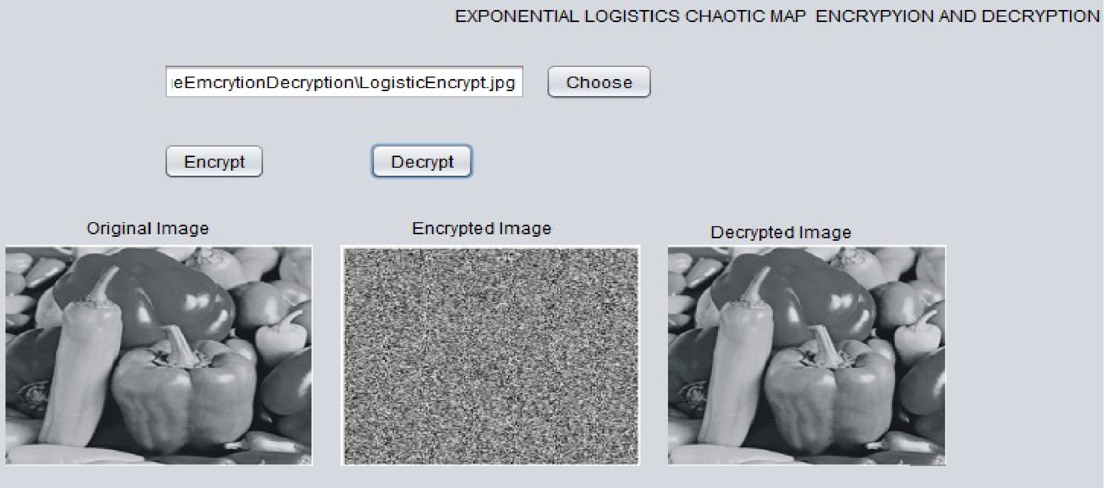
Below are the results of the simulations of the digital image encryption algorithm using 1-dimensional exponential logistic map.



ieEmcrytionDecryption\LogisticEncrypt.jpg

Figure 7: Original, encrypted and decrypted gray Lena images using one-dimensional exponential logistic image encryption algorithm.

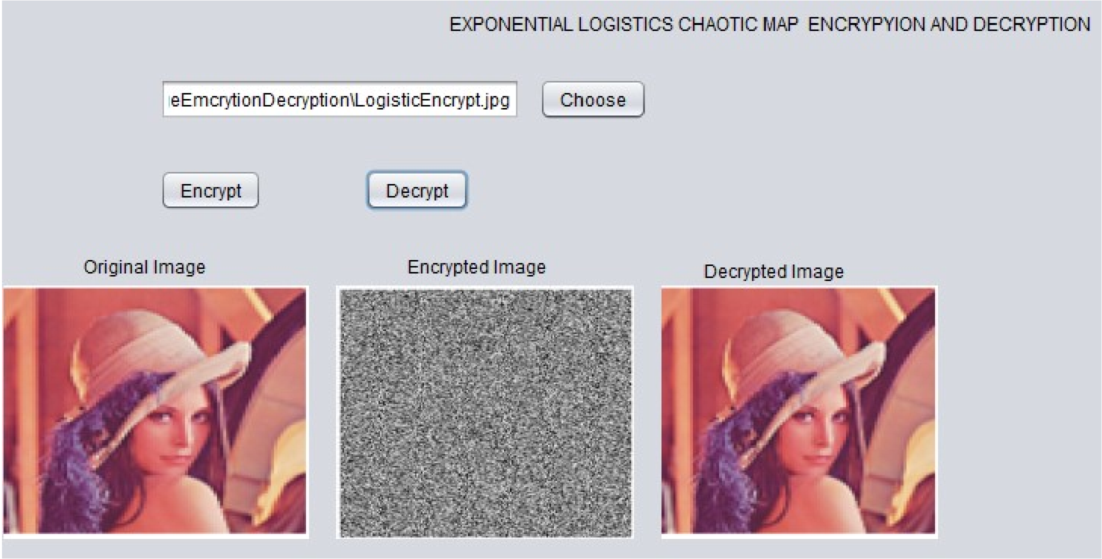
Figure 7 shows the results of original, encrypted and decrypted gray Lena images using one-dimensional exponential logistic image encryption algorithm. The image is chosen from the file, encrypted and decrypted as shown by selecting the encrypt and decrypt buttons as seen in Figure 7.



ieEmcrytionDecryption\LogisticEncrypt.jpg

Figure 8: Original, encrypted and decrypted gray Peppers images using one-dimensional exponential logistic image encryption algorithm.

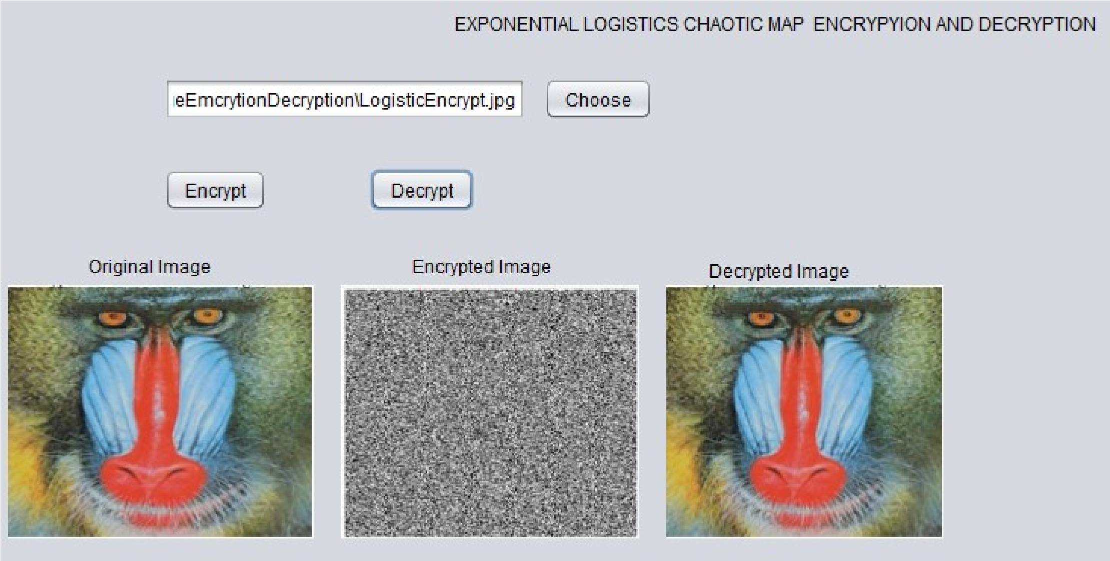
Figure 8 shows the results of original, encrypted and decrypted gray Peppers_ gray images using one-dimensional exponential logistic image encryption algorithm. The image is chosen from the file, encrypted and decrypted as shown by selecting the encrypt and decrypt buttons as seen in Figure 8.



ieEmcrytionDecryption\LogisticEncrypt.jpg

Figure 9: Original, encrypted and decrypted RGB Lena images using one-dimensional exponential logistic image encryption algorithm.

Figure 9 shows the results of original, encrypted and decrypted RGB Lena images using one-dimensional exponential logistic image encryption algorithm. The image is chosen from the file, encrypted and decrypted as shown by selecting the encrypt and decrypt buttons as seen in Figure 9.



ieEmcrytionDecryption\LogisticEncrypt.jpg

Figure 10: Original, encrypted and decrypted RGB Mandril images using one-dimensional exponential logistic image encryption algorithm.

Figure 10 shows the results of original, encrypted and decrypted RGB Mandril images using one-dimensional exponential logistic image encryption algorithm. The image is chosen from the file, encrypted and decrypted as shown by selecting the encrypt and decrypt buttons as seen in Figure 10.

Conclusion

The simulation results showed that the proposed chaotic image encryption algorithms had high operation efficiency and good encryption effect. The presented algorithm showed superiority over other algorithms in terms of processing time and protection. We therefore conclude that the modified one-dimensional exponential logistic map image encryption algorithm can withstand various forms of attacks ensuring for confidentiality and security. Thus, the new maps is suitable for image encryption and can be used for real time applications.

Declaration of conflicting interests

The authors declared no potential conflicts of interest

References

[1] Farouzan, B.A. (2010). *TCP/IP Protocol Suite. 4th Edition.* , Boston: McGraw Hill. 667pp.

[2] Huang, C.K., Liao, C.W., Hsu, S.L. and Jeng, Y.C. (2012). Implementation of Grey Image Encryption with Pixel Shuffling and Grey-Level Encryption by Single Chaotic System. *Telecommunication System.* **10**(1): 247-256.

[3] Lee, C. and Chen, T. (2003). A New Encryption Algorithm for Image Cryptosystem. *Cite SeerX.* **1**:1-10.

[4] Stallings, W. (2006). *Cryptography and Network Security: Principles and Practices; 4th Edition.* New Jersey: Prentice Hall.500pp.

[5] Jikmoski, G. and Kocarev, L. (2001). Chaos and Cryptography: Block Encryption Ciphers Based on Chaotic Maps. *Circuits and Systems I: Fundamental Theory and Applications, IEEE Transactions.* **48**(2):163-172.

[6] Effa, J.Y., Nkapkop, J.D., Borda, M., Bitjoka, L., Mohamadou, A. (2016). A Secure and Fast Chaotic Encryption Algorithm Using the True Accuracy of the Computer. *Informatica***40** (2): 437-445.

[7] Alvarez, G. and Li, S. (2006). Some Basic Cryptographic Requirements for Chaos-Based Cryptosystems. *International Journal of Bifurcation and Chaos.* **16**: 2129-2151.

[8] Biswas, R.H. (2013). One Dimensional Chaotic Dynamical Systems. *Journal of*

and Applied Mathematics: Advances and Applications. ***10****(1)*:69-101.

[9] Baker, G.L. and Gollub, J.P. (1990). *Chaotic Dynamics an Introduction.* New York: Press Syndicate of the University of Cambridge. 550pp.

[10] Auyporn, W. and Vongpradhip, S. (2015). A Robust Image Encryption Method Based on Bit Plane Decomposition and Multiple Chaotic Maps. *International Journal of Signal Processing Systems.* **3**(1):8-13.

[11] Kaur, S. and Gupta, D. (2016). A Review of Image Encryption Schemes Based on the Chaotic Map. *International Journal of Computer Technology and Applications* .**5**(1):144-149. Retrieved from www.ijcta.com on 1st March, 2017.

Cite this article

Gbaden T. and Gbaden A.R. (2021). Digital Image Encryption and Decryption . *FUAM Journal of Pure and Applied Science,***1**(**1**): 71-80