Advances in Mathematical & Computational Sciences Journal,
Vol. 7 No. 1, March 2019

Article Citation
Format Ikuomola, A. J. (2019): Securing Digital Image using Chaotic Encryption Scheme.
Journal of Advances in Mathematical & Computational Sciences
Vol. 7, No. 1. Pp 1-10

Article Progress Time Stamps
Article Type: Research Article
Manuscript Received 11th Dec. 2018
Review Type: Blind
Final Acceptance: 7th January, 2019
Article DOI: dx.doi.org/10.22624/AIMS/MATHS/V7N1P1

Securing Digital Image using Chaotic Encryption Scheme

Aderonke J. Ikuomola
Department of Mathematical Sciences,
Ondo State University of Science and Technology
Okitipupa, Nigeria
E-mail: deronikng@yahoo.com, aj.ikuomola@osustech.edu.ng

ABSTRACT

Encryption of images is different from that of texts due to some basic features of images such as bulk data capacity and high redundancy, which are generally difficult to handle by traditional means. Most of the available ciphers cannot be used directly to encrypt digital images in real-time systems because their encryption speed is not fast. In this paper, a chaotic image encryption schemes which uses a two-dimensional discretized Arnold's cat map was used for pixel permutation and a logistic map which is a one-dimensional chaotic map was used for key stream generator where the control parameter b is used as part of the secret key. The work was implemented using Microsoft Visual Basic 2008. The result shows an encrypted image which is decrypted by inverse of the map and the use of the secret keys. The chaotic system employed shows its simplicity in form and complexity in dynamics.

Keyword: Arnold's Cat Map, Cryptography, Chaotic, Digital Image, Logistic Map.

1. INTRODUCTION

After the advent of internet, security of digital image data which is transmitted over all kinds of wired or wireless channels and protection of privacy has become major concerns. In addition, special and reliable security in storage and transmission of digital images are needed in many digital applications, such as pay-TV, confidential video conferencing and medical imaging systems [9]. A developed modern cryptography should be the best solution and the advances in digital communications technology have provided a way of designing new efficient encryption schemes. In Cryptography, encryption is the process of transforming information (referred to as plaintext) using an algorithm (called cipher) to make it unreadable to anyone except those possessing special knowledge, usually referred to as a key. Cryptography is one technique used in securing digital data. Cryptography does not hide message but instead scrabble the message through an encryption process to produce an unreadable cipher text. One of the objectives of cryptography is to preserve the information secrecy from all except the ones the information is intended for, which is privacy and confidentiality.

Image Encryption is an extremely useful method for stopping unwanted interception and viewing of any transmitted image or other information. However, the traditional text encryption schemes fail to protect image data efficiently due to the big differences between image data and text, such as strong redundancy existing in uncompressed image data and its bulky size [8]. Traditional image encryption algorithm such as data encryption standard (DES) has weakness of low-level efficiency when the image is large [3][11][4]. Also, Internationally Data Encryption Algorithm (IDEA) and Rivest Code 5 (RC5) which are widely used today may not be suitable for multimedia applications due to its large data sizes and real time constraints.

According to [7] principle of secure cryptosystem, the security should depend on the secrecy of the key, not the secrecy of the encryption/decryption algorithm that was used. In other words, it is assumed that the algorithm is publicly known, yet decryption of message is infeasible on the basis of the cipher text in addition to knowledge of the algorithm. Thus, to protect the content of digital images, some chaotic encryption systems are needed. Chaotic systems have may important properties, such as the sensitive dependence on initial conditions and system parameters, pseudorandom property, non-periodicity and topological transitivity, etc. Most properties meet some requirement such as diffusion and mixing in the sense of cryptography [17]. The Chaos-based encryption has suggested an efficient way to deal with the problem of fast and highly secure image encryption. Logistic map which is a one-dimensional chaotic system having a high-level efficiency and simplicity has been widely used but it is weak because it has small key space and weak security.

In order to overcome these drawbacks, this paper presents a Chaotic Image Encryption System (CIES), which is based on Chaotic Logistic map and Arnold's Cat map. The combination of the two maps helps to improve the security of this scheme. In the rest of this paper, section 2 presents the review of related works done on securing digital image, Section 3 describe the technique employed in the design of a Chaotic Image Encryption System (CIES). Section 4 and 5 describe the implementation and conclusion respectively.

2. LITERATURE REVIEW

[9] proposed a novel video encryption scheme based on multiple digital chaotic systems, which is called CVES (Chaotic Video Encryption Scheme). CVES is independent of any video compression algorithms, and can provide high security for real-time digital video with fast encryption speed, and can be realized both by hardware and software. CVES can be extended to support random retrieval of cipher-video with considerable maximal time-out; the extended CVES is called RRS-CVES (Random-Retrieval-Supported CVES.

[13] proposed methods for encrypting medical image data selectively in special domain and frequency domain respectively. These proposed methods were further analyzed and improved on by [1]. [6] presents a nonlinear chaotic algorithm (NCA) which uses power function and tangent function instead of linear function. [12] proposed an efficient joint compression and selective encryption scheme which was based on set partitioning in hierarchical trees of wavelet coefficients. The confidentiality of image was achieved by encrypting only the significance bits of individual coefficients. A scheme that uses a secrete key and a mapping function to generate a private initial table to encrypt the selected DWT code blocks in the entropy coding state of JPEG 2000 was proposed by [10]. [14] uses two Logistic maps to generate pseudo-random number sequences to determine complex combination of some simple basic operations including XOR, modulo addition and modulo subtraction.

[9] studied the security of the scheme proposed by [14] and discovered that there exit number of problems with the secret key and that the scheme can be broken with a chosen-plaintext attack. In [15], the value of every pixel of plain-image is converted into the initial condition of Logistic map and the value obtained by iterating the map was used to mask the value corresponding to neighboring pixel. [2] analyzed the scheme proposed by [15] and then improved on the security of this scheme.

In [5] in order to effectively realize digital image encryption and decryption, two one-dimensional discrete Chebyshev chaotic sequences are used for row and column scrambling of the pixels of original and encrypted digital images. [16] proposed a chaotic maps-based key agreement protocol that will not only fix the weaknesses of the existing chaotic maps-based key agreement protocols but also aims to preserve user anonymity. The proposed protocol was able to: achieved mutual authentication between a server and a user; allowed users to anonymously interact with the server to agree on session keys; allowed a server and a user to generate session's keys. Petri nets was used in the security analysis of the proposed protocol.

3. DESIGN METHODOLOGY

The model used for designing the Chaotic Image Encryption System (CIES), which is based on chaotic Logistic map and Arnold's Cat map and the architecture of the model are presented in this section.

3.1 The Mathematical Model

Chaotic Image Encryption System (CIES) uses chaotic maps in its process.
The one- dimensional logistic map is used in its key generation.

$$Logisticmap: x_{n+1} = bx_n(1 - x_n) \quad \ldots\ldots\ldots\ldots\ldots\ldots \quad equation\,(i)$$

where:
b is the control parameter governing the chaotic behavior, which has a value that lies between 1 and 3
x_n which is the initial value of x is the secret key specified in the CIES interface.
The logistic map is iterative. The first iterative value, that is x_{n+1} is assigned to control parameter *a*, the second iterative value, that is x_{n+2} is assigned to control parameter *b* used in the permutation phase.

The two-dimensional parameterized Arnold's cat map is used in its permutation phase.

$$Parameterized\ Cat\ map: \begin{pmatrix} x_{n+1} \\ y_{n+1} \end{pmatrix} = \begin{pmatrix} 1 & a \\ b & ab+1 \end{pmatrix} \begin{pmatrix} x_n \\ y_n \end{pmatrix} \quad \ldots\ldots\ldots\ldots \quad equation\,(ii)$$

$$The\ linear\ eauation\ gives \quad x_{n+1} = x_n + ay_n \quad \ldots\ldots\ldots\ldots\ldots\ldots \quad equation\,(iii)$$
$$y_{n+1} = bx_n + (ab+1)y_n$$

where:
x_n is the initial position of the pixel on the x axis of the image
y_n is the initial position of the pixel on the y axis of the image
x_{n+1} is the relocated position of the pixel on the x axis
y_{n+1} is the relocated position of the pixel on the y axis
a is a control parameter
b is a control parameter

3.2 Encryption Engine

Step1: Browse for the image
Step2: Load the selected image into the picture box
Step3: Specify a key in the text box, ***k*** and the value of ***b*** to be used also as the key.
Step4: Encrypt the image
Generating a, b, then x_{n+1}, y_{n+1} to relocate the pixels.
Step5: The encrypted image is displayed in the picture box and the conversion time is displayed.
Step6: The encrypted image is saved.

3.3 Decryption Engine

Step1: Fetch the encrypted image from the stored location
Step2: Specify the same keys used in encryption in the text boxes provided
Step3: Decrypt the image
Step4: The decrypted image is displayed and the conversion time is displayed.

3.4 Architecture of Chaotic Image Encryption System

Figure 1 shows the Architecture of Chaotic Image Encryption System. For the encryption and decryption, the value entered by the user in the interface (secret key) is the initial value of x_n that is used at the key generation phase and the *b* value is also specified by the user. The first value of x_n derived is taken as the value of *a* used in the permutation phase. The next iterative value is taken as the value of *b* also used in the permutation phase. At the permutation phase, *a* and *b* are imported from the key generation phase. (x_n, y_n) in the cat map refers to the initial position of the pixels while when substituted into the cat map linear equation (iii), (x_{n+1}, y_{n+1}) is the resulting pixel location. Decryption process is the inverse.

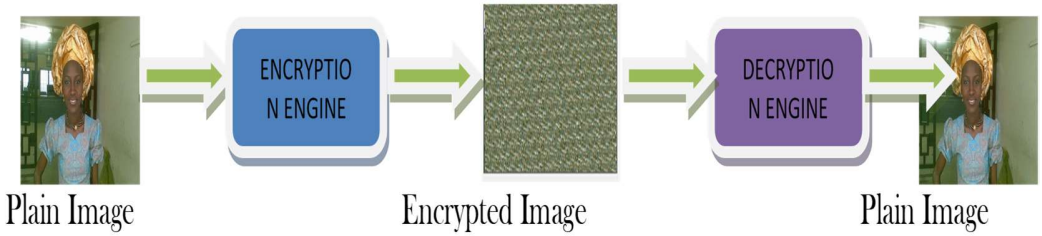

Figure 1: Architecture of the Chaotic Image Encryption System

3.5 Flow Chart of the CIES

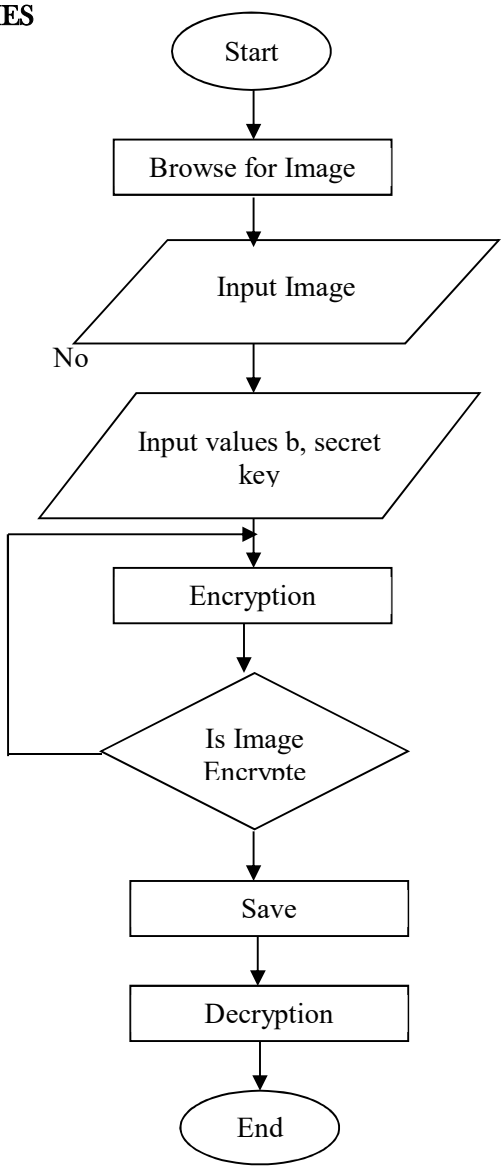

Figure 2: Flowchart of CIES

4. IMPLEMENTATION AND TESTING

The design was run on a Pentium IV, 1GHz Processor computer with 512MB of RAM and at least 5MB free Hard disk space running on Microsoft Windows XP Professional or Vista Operating System. Microsoft Visual Basic 2008 Express edition was used as the programming language for the implementation of the design.

4.1 Interface Design

Figure 3 shows the interface of the Chaotic Image Encryption System (CIES) where the digital image will be uploaded.

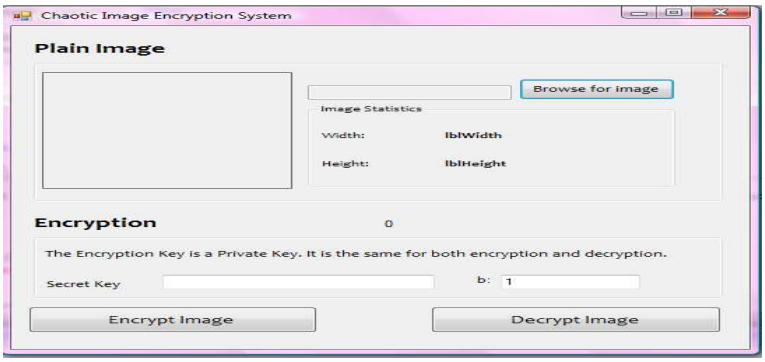

Figure 3: Chaotic Image Encryption System Interface.

The operator browses through the system for the image to be encrypted and loads it. Figure 4 displayed the plain image and the image statistics.

Figure 4: Plain image is loaded

In figure 4 above the secret key and b value are specified, and encryption begins at the press of the button and the time used in the process is displayed while figure 5 shows the encrypted image with the time taken to process the image. The encrypted image is saved in a specified location where it can be fetched when needed.

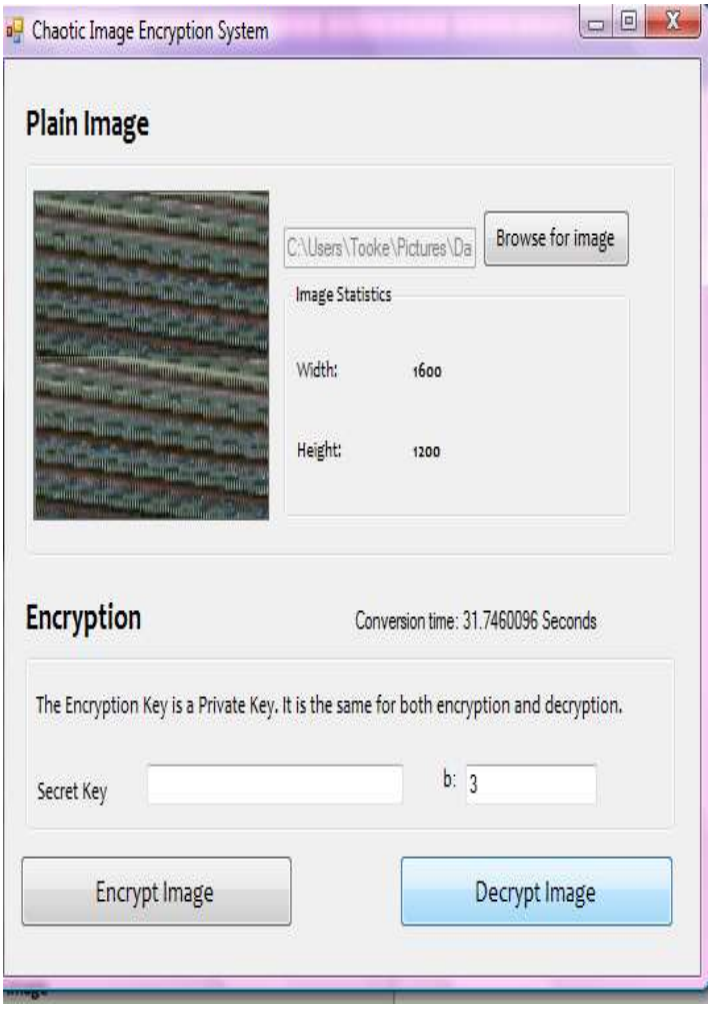

Figure 5: The encrypted image with the time taken

During decryption, the encrypted image is fetched. The same keys used in encryption are also used for the decryption process as shown in figure 6 and the decrypted image with the time taken to decrypt are displayed in figure 7.

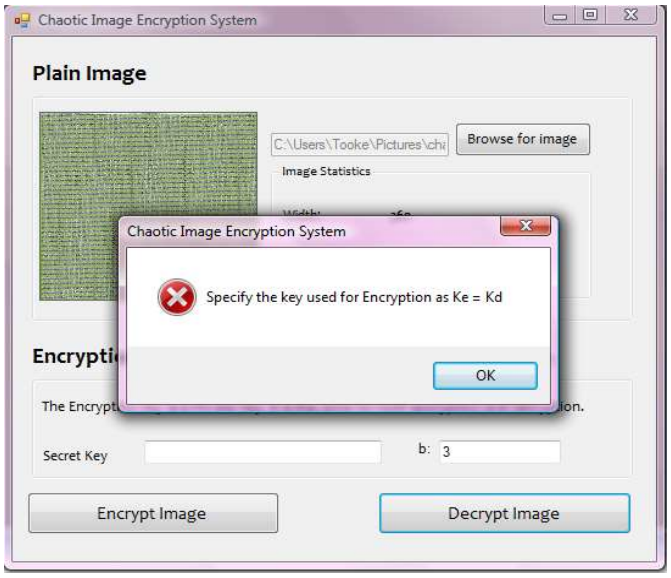

Figure 6: specify the key

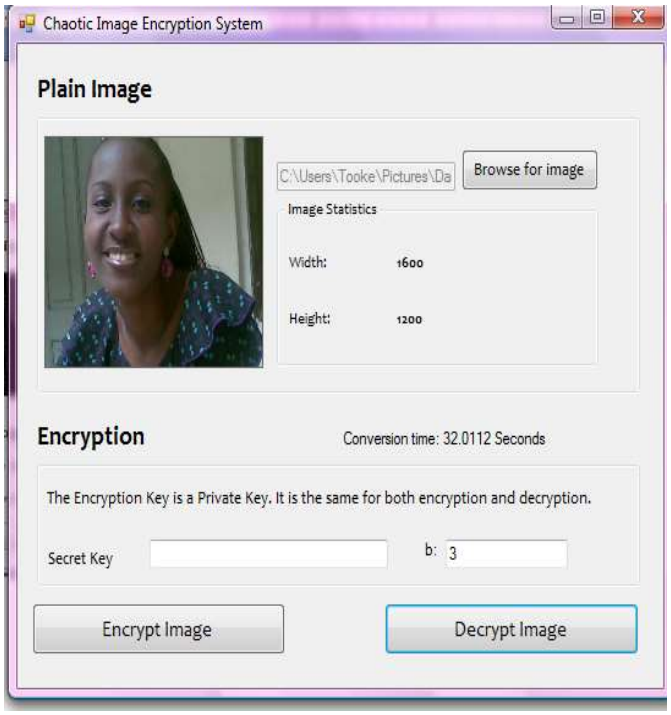

Figure 7: The decrypted image with the time taken.

5. CONCLUSION

Security is one of the biggest threats to digital image data today. The application of cryptography to digital image data is definitely an avenue for reducing the rate of unauthorized access to digital image data. Cryptography algorithms prevent a situation where the confidentiality and integrity of data is being questioned. Traditional cryptographic schemes are mainly based on discrete mathematics composed with many complicated algebraic operations, while chaotic cryptographic schemes rely on the complex dynamics of nonlinear maps which are deterministic but simple.

In this paper, a chaotic image encryption schemes which uses a two-dimensional discretized Arnold's cat map was used for pixel permutation and a logistic map which is a one-dimensional chaotic system having a high-level of efficiency and simplicity was used for key stream generator where the control parameter, b is used as part of the secret key. The encryption scheme is safe and can be used in standard works.

REFERENCES

[1] Alvarez G., Li S. and Hernandez (2007). Analysis of Security Problems in a Medical Image Encryption System. Computers in Biology and Medicine, 37(3), 424-427

[2] Arroyo D. Rhouma R. Alvarez G. Li S. and Fernandez V. (2008). On the Security of a New Image Encryption Scheme based on Chaotic Map Lattices

[3] Chen G., Mao Y., and Chui C.K., 2004 A symmetric image encryption scheme based on 3D chaotic cat map, *International Journal of Bifurcation and Chaos*, 14(10).

[4] Chiaraluce F. , Ciccarelli L. (2002). A New Chaotic Algorithm for Video Encryption. IEEE Trans Consum Electron, 48:838-843.

[5] Dinghui Z., Qiujie G, Yonghua P. and Xinghua Z. (2008). Discrete Chaotic Encryption and Decryption of Digital Images. 2008 International Conference on Computer Science and Software Engineering

[6] Gao H. Zhang Y. Liang S., LimD. (2006). A New Chaotic Algorithm for Image Encryption. Chaos, Solitons & Fractals, 29: 393-399

[7] Kerckhoff (1964). Cryptographie Militaire, Journel des Sciences militaries, 9th series, IX, English trans. by Warren T. McCready of the University of Toronto

[8] Li C, and Lo K. 2009. Security Analysis of a Binary Image Permutation Scheme based on Logistic Map. *Department of Electronic and Information Engineering, The Hong Kong Polytechnic University, Hong Kong, China*

[9] Li C. Li S. Nunez J. Alvarez G. and Chen G. (2007). On the Security of an Image Encryption Scheme. IACR's Cryptography ePrint Archive: Report 2007/108, available online at http://ePrint.iacr.org/2007/108.

[10] Liu J.L. (2006)"Efficient Selective Encryption for JPEG 2000 Images using Private initial table. Pattern Recognition, 39(8), 1509-1517

[11] Mao Y.B., Chen G. and Lian S.G., 2004. A Novel Fast Image Encryption Scheme Based on the 3D Chaotic Baker Map, Int. J. Bifurcat. Chaos 14(10), 3613-3624.

[12] Martin K. Lukae R. and Plataniotis K. N. (2005). Efficient Encryption of Wavelet-based Coded Color Images. Pattern Recognition, 38(7), 1111-1115.

[13] Noreen R., Podesser, Pommer A, Schmidt A. Uhl A. (2003). Confidential Storage and Transmission of Medical Image Data. Computers in Biology and Medicine, 33(3), 277-292

[14] Pareek N. Patidar V. and Sud K. (2006). Image Encryption using Chaotic Logistic Map. Image and Vision Computing, 24(9), 926-934

[15] Pisarchik A. N. Flores-Carmona N.J. and Carpio-Valadez M. (2006). Encryption and Decryption of Images with Chaotic Map Lattices. Chaos, 16(3).

[16] Tseng H., Jan R. and Yang W. (2009). A Chaotic Maps-based Key Agreement Protocol that Preserves Uset Anonymity. IEEE ICC'2009 International Conference on Communications (Ad hoc and Sensor Networking Symposum).

[17] Zhang L.H., Liao X. F., and Wang X.B. (2005). An image encryption approach based on chaotic maps," Chaos, Solitons & Fractals, 24:759-765