International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 9 Sep. 2022, pp: 250-254 www.ijaem.net ISSN: 2395-5252

Optimizing Symmetric vs. Asymmetric Image encryption mathematically

Baydaa Jaffer Al-Khafaji[1, a]
Prof. Abdul Monem S. RahmaPh.D[2, b]

Iraqi Commission for Computers and Informatics ,Informatics institute for postgraduate studies, Baghdad, Iraq[1]
Computer Science Department, Al-Maarif University College, Iraq,[2]

Date of Submission: 01-09-2022 Date of Acceptance: 10-09-2022

ABSTRACT
In recent years, communications via Internet are getting more frequent with the increasingly wide reach of the Internet. Dueto a large number of threats against communications security,protection of information has become an important issue.Especially because digital images contain large amount of information, security for images is a major concern. Many applications like Medical imaging, Military image databases, videoconferencing, online photograph album, etc. require security system which is reliable and robust to store and transmit digital images.Chaotic cryptologyis the application of the mathematical chaos theory to the practice of the cryptography,the study or techniques used to privately and securely transmit information with the presence of a third-party or adversary.
The requirements to full the security needs of digital images have led to the development of good encryption techniques. The digital images have certain characteristics such as being less sensitive as compared to the text data as a tiny change in the attribute of any pixel of the image does not drastically degrade the quality of the image and bulk capacity of data, redundancy of data, strong correlation among adjacent pixels, etc. The main objective of the Search is Image encryption is an effective approach to protect images by transforming them into completely different formats. Which are used to protect the confidential image data from any unauthorized access using chaotic algorithm to increase protect images
Keywords:chaotic algorithm**,** Image encryption,H´enon map ,HolmesMap, Asymmetric, Symmetric

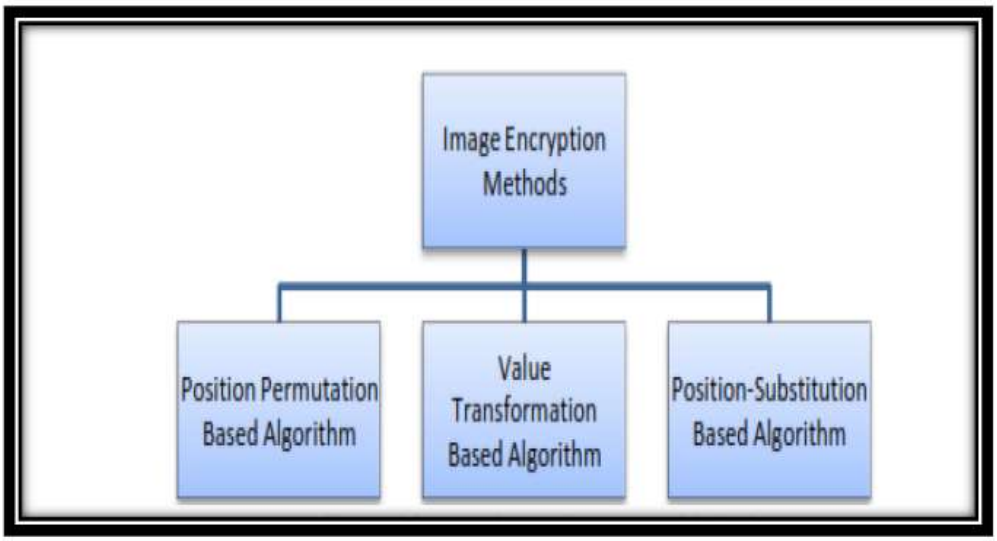
I. INTRODUCTION

With the increasing growth of multimedia applications, security is an important issue in transmission of images. Encryption is one the way to ensure security[1]. Image encryption techniques convert original image to another image which is hard to understand[4]. Encryption is the process of encoding messages or information in such a way that only authorized parties can able to read it using the decryption key[2][4]. An authorized person can easily decrypt the message with the key provided. Somebody who is not authorized can be excluded, because he or she does not have the required key, without which it is impossible to read the encrypted information. The purpose of image processing is divided into several groups[4][3].

Encryption Objectives
1. Confidentiality: is a service used to store the information content ofall persons except those who have been authorized to view it.
2. Data Integrity: A service used to save information from change(delete, add or modify) by unauthorized persons.
3. Identifying identity: a service used to prove the identity of data handling (authorized).
4. Non-Repudiation: A service or function that prevents any entity from denying any previous undertaking or work done so when such dispute occurs between the parties involved in the denial of its actions, then a specific means of resolving this dispute shall be provided. Through a specific procedure involving a trusted third party[2][4]

Various Image Encryption Methods:
There are various types of image encryption methods. The image encryption algorithms can be categories into three major groups.[5][6][7]

International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 9 Sep. 2022, pp: 250-254 www.ijaem.net ISSN: 2395-5252



Various Image Encryption Methods.

Chaotic algorithm

The remarkable importance of chaotic iterated maps in both modeling and information processing in many fields explains the need for their hardware analog and digital realizations, e.g., Since we are concerned with digital implementations, we present a review of several studies that have been conducted on the effect of finite-precision on the properties of chaotic systems and are much related to our proposed work[7]. The problem of simulating or implementing digital chaos is composed of two parts: finite time and finite precision. This implementation is done probably in some sort of digital calculations on computers. In this case, sentences like steady state or the limit as the number of discrete time steps approaches infinity no longer carry the same meaning[8]. Practically, we can only record the behavior of a limited number of time samples: hundreds, thousands, or even millions, but there is no "infinite" time. The same applies to precision, there is nothing practical that is equivalent to infinite precision[9][10].

Chaos-based cryptography has been dividedinto two major groups:

Symmetric chaos cryptography, where the same secret key is used by sender andreceiver.[11][12][13]

Asymmetric chaos cryptography, where one key of the cryptosystem is public.

Chaos: Motivation and Mathematical Analysis:

Chaos theory is a branch of mathematics, which is still in the process of development, classified under the category "applied mathematics to physical sciences". Strange attractors, deterministic models, sensitivity to initial conditions, and fractals are all inherent to the development of this theory. All categories of applied mathematics are always in a state of continuous development in order to find their way towards formulating recent applications either theoretically or practically. However, the history of chaos theory goes back to the 17th century when there have been many arguments and debates whether every effect that is noted on a certain experiment or when observing natural phenomena can beprecisely owed to a given reason or perhaps a list of reasons. Many of these experiments and phenomena can be described by dynamical systems, i.e., their modeling equations relate a quantity to its rate of change, and these are studied as deferential equations. As a result, calculus that is classified under the category of pure mathematics is employed as a powerful tool used in investigating, understanding, and describing "change" in natural sciences and phenomena. The study of chaos enables mathematicians and physicists to describe various phenomena in the field of dynamics by the aid of equations and models.

Chaos theory precisely describes many of the dynamical systems which exhibit unpredictable, yet deterministic, behavior. Chaotic generators can be classified into discrete time maps and continuous time deferential equations. We focus on discrete time maps, however, the most well-known continuous time chaotic Lorenz attractor must be includedwhen handling chaos theory. Other continuous time deferential equations that exhibit 8 chaotic behavior exist such as: Duffng equation. For each generator included in table above, the

International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 9 Sep. 2022, pp: 250-254 www.ijaem.net ISSN: 2395-5252

number of space dimensions, the popular parameter values used to generate chaotic behavior, as well as the characterizing plot that describes the system response are shown in Fig. For 1D maps, the plot presents the map equation or the current iteration xn+1 as a function of the previous iteration xn, in addition to the orbit diagram which shows how the steady state solution varies with respect to the system parameter. Examples for 1D maps are: the logistic, tent, and gauss maps. For two dimensional maps, such as H´enon map and Duffng map, the graph shows one of the involved space dimensions as a function of the other in addition to the orbit diagram.

Finally, respectively. In our study, we concentrate on 1D discrete maps,specifically the logistic and tent maps whose properties are closely relatedsince they are conjugate maps . But at first, a historical background aboutthe development of chaos theory is presented.

Classification of chaotic generators

Map	Space dimensions	Equation(s)	Parameter values
Logistic map	1	$x_{n+1} = \lambda x_n(1-x_n)$	$\lambda = 4$
Tent map	1	$x_{n+1} = \mu \min(x_n, 1-x_n)$	$\mu = 2$
Gauss map	1	$x_{n+1} = e^{-\alpha x_n^2} + \beta$	$\alpha = 6.2, \beta = -0.5$
Hénon map	2	$x_{n+1} = 1 - ax_n^2 + y_n$ $y_{n+1} = bx_n$	$a = 1.4$ $b = 0.3$
Duffing map	2	$x_{n+1} = y_n$ $y_{n+1} = -bx_n + ay_n - y_n^3$	$a = 2.75$ $b = 0.2$

(a) Discrete time maps

Equation	Space dimensions	Equation(s)	parameter values
Lorenz attractor	3	$\dot{x} = \sigma(y-x)$ $\dot{y} = x(\rho - z) - y$ $\dot{z} = xy - \beta z$	$\sigma = 10$ $\rho = 28$ $\beta = 8/3$
Rössler attractor	3	$\dot{x} = -y - z$ $\dot{y} = x + ay$ $\dot{z} = b + z(x-c)$	$a = 0.2$ $b = 0.2$ $c = 5.7$

(b) Continuous time differential equations

Experiment and result

International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 9 Sep. 2022, pp: 250-254 www.ijaem.net ISSN: 2395-5252

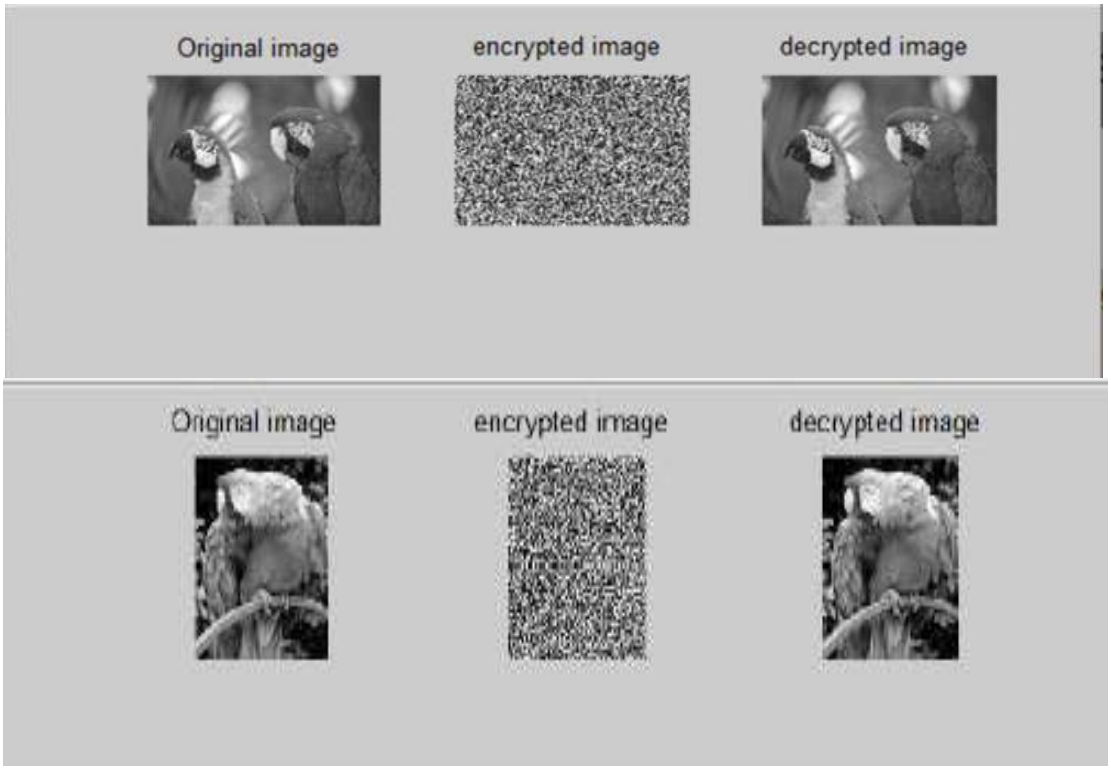


Image	Encryption time	Decryption time
1	**0.003411 sec.**	**1.233334 sec**
2	**0.002054 sec**	**0.132880 sec**
3	**0.005668 sec**	**1.442690 sec**

II. CONCLUSION:

There are a number of conclusions that we came out after completion of the research in both theoretical and practical, which can be summarized as follows:

1 - The proposed algorithm achieves fast and efficient nutrition.

2 - Determine the objectives to be achieved through the current work and modify them according to time requirements is very important to complete the work within the specified period.

REFERENCES

[1]. Xie, Eric Yong; Li, Chengqing; Yu, Simin; Lü, Jinhu (2017-03-01). "On the cryptanalysis ofFridrich's chaotic image encryption scheme". Signal Processing. 132: 150–154.

[2]. B.J AlKhafaji, M Salih, S Shnain, Z Nabat ,improved technique for hiding data in a colored and a monochrm images,2020, Periodicals of Engineering and Natural Sciences 8 (2), 1000-1010

[3]. Li Nan, Sun Caixin, Li Jian, Du Lin, Wang Youyuan. Chaos and Its Application Research Progress in Electric Power Engineering. Journal of Chongqing University(natural science edition), 2005, 28(6): 30-36.

[4]. B.J AlKhafaji, M Salih, S Shnain, Z Nabat,segmenting video frame images using genetic algorithms,2020 Periodicals of Engineering and Natural Sciences 8 (2), 1106-1114

[5]. Akhavan, A.; Samsudin, A.; Akhshani, A. (2015-09-01). "Cryptanalysis of "an improvementover an image encryption method based on total shuffling"". Optics Communications. 350:

[6]. Li, C. (January 2016). "Cracking a hierarchical chaotic image encryption algorithm based onpermutation". Signal Processing. 118: 203–210.

[7]. B.J AlKhafaji, MA Salih, SAH Shnain, OA Rashid, AA Rashid, MT Hussein,2021, Applying the Artificial Neural Networks with Multiwavelet Transform on Phoneme recognition ,Journal of Physics: Conference Series 1804 (1), 012040.

[8]. Ma Youjie, Yang Haishan, Zhou Xuesong, Li Ji, Wen Hulong. Voltage Stabil ity Analysis of Wind Power System. Pro ceedings of the CSU-EPSA, 2010, 22(3): 22-26.

[9]. Jia Hongjie, Yu Yixin, Li Peng, Su Jifeng. Relationships of Power System Chaos and Instability Modes. Proceedings of the CSEE, 2003, 23(2):

[10]. Li Weidong, Wang Xiuyan. Survey on Chaos Control. Techniques of Automation and pplications. 2009, 28(1): 1-5.

[11]. Zhang Weinian, ZhangWeidong. Chaotic Oscillation of a Nonlinear Power System. Applied Mathematics and Mechanics, 1999, 20(10).

[12]. G. Chen. Chaos: Control and anti-control. IEEE Circuits and Systems Society Newsletter, 1998, 9(1).

[13]. RAHMA, A.M.S., RAHMA, M.A.S., and RAHMA, M.A.S. (2015) Automated analysis for basketball free throw. In: Proceedings of the 7th International Conference on Intelligent Computing and Information Systems, Cairo, December 2015. Piscataway, New Jersey: Institute of Electrical and Electronics Engineers, pp. 447-453.