# *Encrypt images using chaotic depending on the intensity and location of the pixel*

# تشفير الصور باستخدام طريقة الفوضى بالاعتماد على شدة وموقع بكسل

**Prof. Dr. Ziad M. Abood**
**Zainab M. Essa**
**Al-Mustansriyh University- College of Education- 2016**

**Abstract**

In any communication, security is the most important issue in today's world. The information security has become one of the most significant problems in data communication. Lots of data security and data hiding algorithms have been developed in the last decade. Cryptography and steganography are the two major techniques for secret communication. In this paper, the secret text is first encrypted by using chaotic which has very good performance and is a most powerful technique. Now this encrypted text is embedded using LSB method. Our proposed system gives two stages of security for secret. The main aim of proposed method to increase security of embedding and extraction phase using chaotic encryption, steganography and change pixel. In order to evaluate performance the proposed algorithm performs series of tests. These tests include, PSNR and MSE.

***Keywords****: Cryptography, Steganography, chaotic.*

**المستخلص:**

يعد عامل الأمنية في أي اتصال من أهم العوامل المهمة في وقتنا الحالي. أصبح أمن المعلومات واحدة من أهم المشاكل في نقل البيانات. وقد وضعت الكثير من أمن البيانات والمعلومات وخوارزميات الاخفاء في العقد الماضي. يعد التشفير وإخفاء المعلومات نوع ان من التقنيات الرئيسية للاتصالات السرية دون الكشف عن المعلومات المنقولة. في هذه الدراسة، تم تشفير نص السريل أول مرة باستخدام نظرية الفوضى التي تمتاز بأداء قوى وصعب عن طريق تشفير نص مشفرة باستخدام طريقة LSB .

والهدف الرئيسي من الطريقة المقترحة هي زيادة الأمن في اخفاء وتشفير المعلومات ثم مرحلة استخراج باستخدام التشفير الفوضى، إخفاء المعلومات وتغيير موقع بكسل للصورة التي استخدمت كغطاء للاخفاء المعلومات. وتم حساب PSNR وmse من أجل تقييم أداء الخوارزمية المقترحة.

## 1- Introduction

Since the beginnings of human information transfer, the wish to communicate in secrecy has existed. Whether planning a surprise birthday party or overthrowing a government, exchanging information in secret is essential. There has been multi solutions to this problem, the most usually used and investigated being “cryptography” [1].Historically, sensitive data has been protected using encryption. Encryption uses powerful mathematics to convert plaintext into an unreadable cipher text that is transmitting over a channel to the recipient [2]. When a message is encrypted it is done so using a “secret key”. To decrypt a message, the secret key is used to reverse the operation. For an ease dropper to defeat the system he or she must get the secret key. Typically it is supposed that this must be done by searching through the entire key space; a so

called “brute-force” attack. As this is a very time consuming endeavor, the “encrypted message” is considered safe [1][3]. Second method of information transfer, called “steganography” is the art of hiding information in ways that prevent the detection of hidden messages. It includes a vast array of secret communication methods that conceal the very existence message. Steganography has its place in security. It is not intended to replace cryptography but supplement it. Hiding a message with steganography methods reduces the chance of a message being detected. If the message is also encrypted then it provides another layer of protection. Therefore, some stenographic methods combine traditional cryptography with steganography, the sender encrypts the secret message prior to the overall communication process, as it is more difficult for an attacker to detect embedded cipher text in a cover. Consequently strong steganography systems do not need prior encryption stage [4].

**2- Chaotic System**

A chaotic system is a nonlinear deterministic dynamical system which exhibits pseudorandom behavior. The output values of chaotic systems vary depending on specific parameters and initial conditions. Different parameter values yield different periods of oscillations at the output of the systems [5].

Signalsof chaotic are cannot be very predictable and “random-likenature”, that more attraction characteristic of “deterministic chaotic systems”it could lead tonovel (engineering) applications. A few of the common characteristics

between “chaos andcryptography” are being sensitive to “variables and parameters changes”. The significant dissimilarity between “chaos and cryptography”located on the fact,“chaos” use the system are recognized only on “real numbers”, however“cryptography” use the system are recognized on “finite numberof integers”. Though, therefore we believe that thedisciplines learned from each other. [6] A chaotic map is a function of its domain and range in the same space, andthe starting point of the trajectory is called the “initial value (condition)”. Chaotic dynamics have a uniqueattribute that can be seen clearly by imagining the system starting twice with slightly different initial conditions. Chaos theory attempts to explain the result of a system that is sensitive to initial conditions, complex, andshows unpredictable behavior. [7] The following types of chaotic map: Logistic Map, Henon Map and Lorenz System.

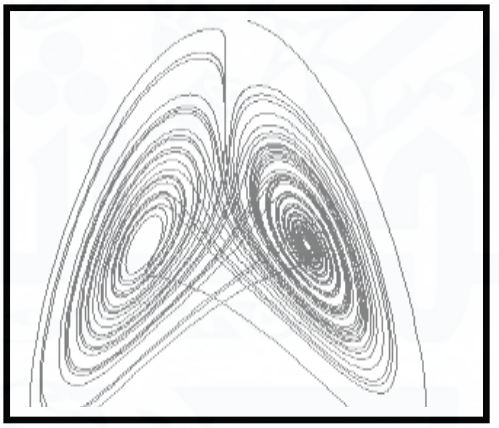

**Fig.1 The chaotic attractor of Lorenz when (a= 10, r = 28, b= 8/3, x=0.000992, y=1 and z=0.000993).**

**Steganography with Images**

The “stego-image” is last product after secret message is inserted in “cover object”. Secret message will be hidden in a “cover-image” by applying an inserted algorithm to create a “stego-image”. The transfer of the “stego-image” via a communication channel is implemented via a sender to a receiver. [8, 9] To show up the covert message that is hidden via the sender, the receiver wants to have the de-stego algorithm which is parameterized via a “stego-key” to abstract the secret message. That is the purpose of a “steganographic” system where an attacker who does not holding the “stego-key” or the name of file to accessing it absolutely will not be capable to decide whether the file is even present. [10] In an effectual “steganographic system”, a typical cover medium should not be distinguishable from a stegoobject.

“Steganography Mechanism Digital images” has be commonplace and nowhere are these images more prevalent than on the WWW in the Internet. The “digital images” use as a carrier medium is appropriate for hiding data because of their insensitivity for the human visual system (HVS) [12]. that large number for web pages are impressively advanced with “color images” and thus Internet users browsing during the web no longer observe to sites having images or to the downloading of images and information files from the Web. Besides, there is a big number of plenty bits in an image. The plenty bits for an object are those bits that can be changed but the change cannot be visibly noticed via human eyes [13]

**3- The Proposed Method**

This paper provides an overview of the proposed system, presenting the images used in this study and these images on different dimensions and with file format (PNG) and with Color model (CMYK, YIQ). Table (1) contains CMYK images and YIQ.

**Table (1) RGB and HSV images dataset**


#1


#2


#3


#4


#5


#6

**Table (2) Cover images size and models**

| No. images | Size images | Color model |
|---|---|---|
| #1- | 2718*1808 | CMYK |
| #2- | 1280*1024 | CMYK |
| #3- | 2560*1600 | CMYK |
| #4- | 2718*1808 | YIQ |
| #5- | 1280*1024 | YIQ |
| #6- | 2560*1600 | YIQ |

**3-1 Diagram of proposed system**

The proposed system consists of the technique that used encryption text, steganography and change pixel by (cross correlation, Intensity) and images quality calculation as shown in figure (2):

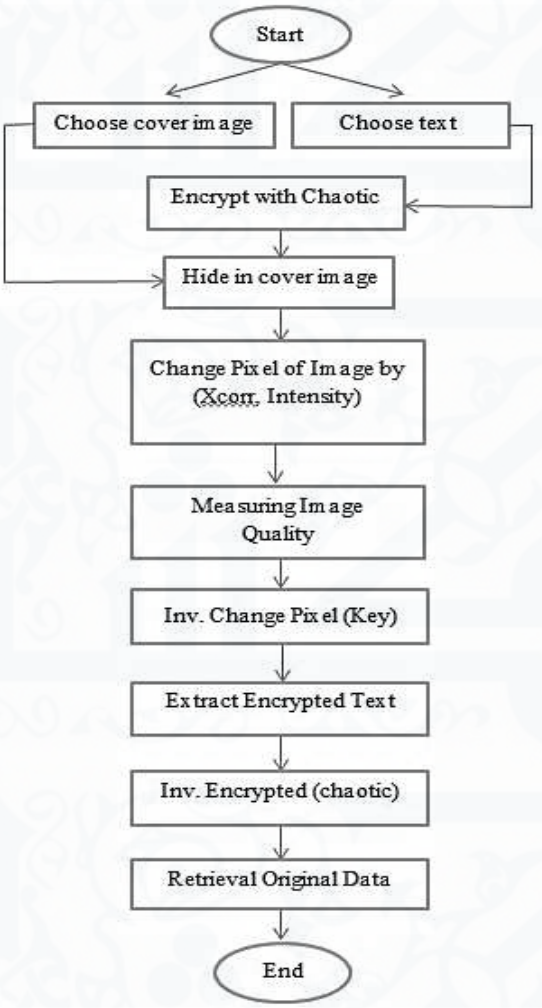


**Fig.2 The proposed system**

## 4- Results and Discussions

It will be review the results that were obtained through the implement chaotic encryption method with LSB and change pixel. Cross correlation in this method, matching region change in two images (stego-image (full), template), must be the full image larger than template image. Change pixel intensity In this method calculate mean, mode and median, for image after divided image to blocks,

these blocks equal size and then add threshold to each block. The performance of the proposed approach has been studded using two kinds of measures (PSNR, MSE). Shows in tables (3, 4):

**Template for CMYK** **Template for YIQ**

**Fig.3 Shows template (CMYK, YIQ)**

**Table (3) CMYK, YIQ cross correlation change**

| Image no. | $PSNR_{RED}$ | $MSE_{RED}$ | Color model |
|---|---|---|---|
| **#1-** | 99 | 0.8247 | CMYK |
| **#2-** | 99 | 1.2303 | CMYK |
| **#3-** | 99 | 1.1231 | CMYK |
| **#4-** | 99 | 0.7130 | YIQ |
| **#5-** | 99 | 1.4740 | YIQ |
| **#6-** | 99 | 0.6171 | YIQ |

**Table (4) CMYK, YIQ threshold change**

| Image no. | $PSNR_{RED}$ | $MSE_{RED}$ | Color model |
|---|---|---|---|
| **#1-** | 27.0312 | 128.8118 | CMYK |
| **#2-** | 26.8829 | 133.2889 | CMYK |
| **#3-** | 26.9928 | 129.9578 | CMYK |
| **#4-** | 26.8819 | 133.3175 | YIQ |
| **#5-** | 26.9840 | 130.2201 | YIQ |
| **#6-** | 26.9295 | 131.8663 | YIQ |

We observed that PSNR of the tested images using the proposed cross correlation change has maximum value (99 dB). MSE of the tested images using the proposed cross correlation change has minimum value (0.6171).

**Conclusions:**

This paper presented a description of increase security. The algorithm is employed effectively over an insecure channel and working against attacks by producing high imperceptible stego-images. Apply chaotic encryption give better result with change pixel (cross correlation, Intensity) depended on measurement results (PSNR and MSE). Chaotic encrypt different size of texts that contains numbers, letters and special character. In additional, used LSB method for hide-encrypted data in cover images with models (CMYK, YIQ), format (PNG**).**

## References


[1] **IkhlasFalihAlsudany," Analysis and Detection of Information Hiding in Digital Images", M.Sc., University of Technology, 2006.**

**[2] Neenu Daniel, Lini Abraham, An improved Color Image Encryption Algorithm with Pixel Permutation and Bit Substitution, IJRET: International Journal of Research in Engineering and Technology Vol. 02 Issue: 11, Nov-2013.**

**[3]Mohammad Ali, AmanJantan, Image Encryption Using Block-Based Transformation Algorithm, IAENG International Journal of Computer Science, vol. 35, issue 1. pp. 15-23, 2008.**

**[4] Najla'aAbdHamza Muhsassan, New Robust Information Hiding Technique, MSc. University of Technology, 2005.**

**[5] Ghada S. Karam, Ziad M. Abood , Rafal N. Saleh,**

Enhancement of Underwater Image using Fuzzy Histogram Equalization, International Journal of Applied Information Systems. Vol 6, No. 6, November 2013.

[6] A. V. Prabu, S. Srinivasarao, TholadaApparao, M.JaganmohanRao, K. BabuRao, Audio Encryption in Handsets, International Journal of Computer Applications, Vol. 40, No.6, February 2012.

[7] Mina Mishra and V. H. Mankar, Message Embedded Cipher Using 2-D Chaotic Map, International Journal of Chaos, Control, Modeling and Simulation (IJCCMS) Vol. 1, No.1, July 2012.

[8] Ziad M Abood, Edges Enhancement of Medical Color Images Using Add Images, IOSR Journal of Research & Method in Education, vol.2, 4, 52-60, 2013.

[9] Mahmoud Maqableh, A Novel Triangular Chaotic Map (TCM) with Full Intensive Chaotic Population Based on Logistic Map, Journal of Software Engineering and Applications, 2015.

[10] Pritha Roy and AsokeNath, New Steganography approach using encrypted secret message inside Audio and Video media, International Journal of Advance Research in Computer Science and Management Studies, Vol. 2, Issue 12, December 2014.

[12] G. Viji and J. Balamurugan, LSB Steganography in Color and Grayscale Images without using the Transformation,Bonfring International Journal of Advances in Image Processing,2011.

[13] C. P.Sumathi1, T. Santanam and G. Umamaheswari, A Study of Various Steganographic Techniques Used for Information Hiding, International Journal of Computer Science & Engineering Survey (IJCSES) Vol. 4, No.6, December 2013.