The Encryption and Decryption of Image File Transfer by Chaos

Chart Rithirun[1], Chanuan Uakarn[2], Anuchit Charoen[3]
Electrical Engineering Dept, Faculty of Engineering,
Kasem Bandit University, Thailand
E-mail: chart.rit@ kbu.ac.th[1]
E-mail: cuakarn@gmail.com[2]
E-mail: anuchit.cha@kbu.ac.th[3]

Received: September 2, 2021; Revised: November 12, 2021; Accepted: November 30, 2021

ABSTRACT

This paper presented techniques and methods for applying mathematical equations and chaos theory for encryption and decryption of image file. Research purposes were 1) to study encryption and decryption of image files with Chaos and Chua's Equation, 2) to study the theory of Chaos and apply it in Image Processing, and 3) to study the methods of encryption and decryption and the complexity of the Chaos number system. Chaos theory of chaotic equations was applied in this study to create a pattern of random numbers. Then arranged them in the form of a matrix array, with the dimensions of this matrix in pixels, equal to the dimension of the image file in pixels to be encrypted for receiving a new image file with a chaos mathematical equation being added. This process created the new image file to be encrypted with a chaos equation. It was the output file for forwarding to anyone. To view this file, it needed decryption the encrypted image files with a decryption key from the sender. If the encryption of the key was incorrect, the sent image could not be viewed. The advantage of the encryption and decryption of image files, with the chaos equation, is not complexity. It will manually generate unique random numbers that can not be duplicated. Therefore, the encryption and decryption have very high data security.

KEYWORDS: Encryption and Decryption, Chaos and Chua's Equation

Introduction

The mathematical models used in this research were from "Smart Communication and Control Systems for Robotic (Pitikhet, 2007), which has studied the chaotic equation and simulate the behavior of various chaotic equations. In this paper, the Chua's chaotic equations were presented.

Chua's equation is a 3D chaotic equation that contains the mathematical equation:

$$\frac{dx}{dt} = a(y - x - f(x))$$
$$\frac{dy}{dt} = b(x - y + z) \quad (1)$$
$$\frac{dz}{dt} = -cy$$

Which

$$f(x) = m_1 x + 0.5(m_0 - m_1)(|x + 1| - |x - 1|)$$

and

$$x_0, y_0, z_0 = [0.1, 0.1, 0.1]$$

then

$$a, b, c = [15.6, 1, 25.58]$$

$$m_0, m_1 = \left[-8/7, -5/7\right]$$

The solution of Chua's equation in the time domain shows as in Figure 1.

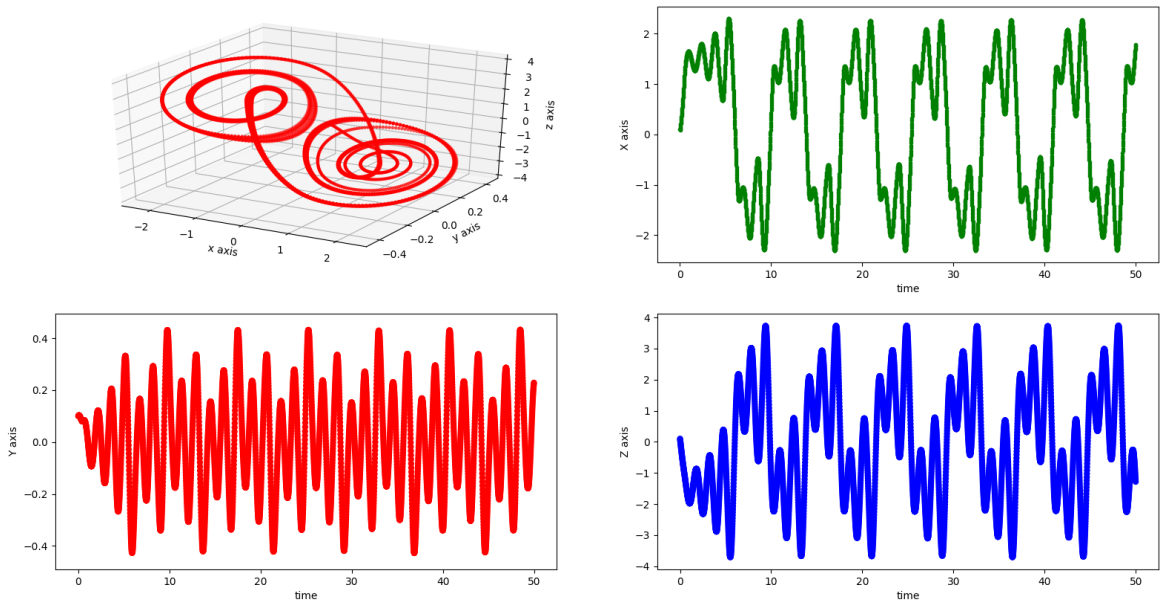


Figure 1 Solution of Chua's equation

Purposes

1. To study encryption and decryption of image file with Chaos and Chua's equation.
2. To study the theory of Chaos and apply it in Image Processing.
3. To study the methods of encryption and decryption and the complexity of the Chaos number system.

Benefit of Research

1. Resulting in knowledge that leads to academic advancement in both mathematical theory that is blended with engineering.
2. It provides a good understanding of Chaos theory to be applied to image file access and decryption.
3. It creates new knowledge that will be useful in modifying, improving or developing cryptography technology and decrypt different data better.

Research Process

1. To determine the size of the image file and the preview image file.
2. Creating a Python program to write the Chaos equations for encoding an image file into an encryption image file.
3. Creating a Python program to rewrite the Chaos equation to decrypt an already encrypted image file to get the original image file back.

Literature Review: Theory

In addition to the equations mentioned above, there are still many chaotic equations that interested people can find in the reference documents (Klomkarn & Sooraksa, 2004). Mathematical models of chaotic equations presented in this project

has been programmed to look at the chaos behavior with various default conditions as previously presented by using Python 2.7 program to write equations and plot graphs (Joseph et al. 2016), (Kenneth & Howe, 2014), the results of the experiment in computer simulations have shown the behavior of restlessness of the equation that has already been presented. Moreover, we developed as encryption an image file in the next section.

Encrypting image files

Digital image files that are delivered to each other in a computer system come in many formats such as JPEG, GIF, PNG, BMP, TIFF etc. The files are presented in this encryption is a raster based digital graphics file commonly known as "Bitmap" which is caused by bringing together several small dots for image X pixel and Y pixel and the depth is Z pixel.

The picture displayed on the computer screen is caused by the operation of the RGB color model, which consists of Red (R), Green (G) and Blue (B) using the principle of emitting an electric charge to change the 3 colors together to cause It is a small rectangular point called a pixel and many pixels are placed next to each other that they will form a picture, this raster graphic must assign a number of pixels to the desired image. If the number of pixels were small when enlarging the image to be larger the picture, it would be seen as a small square box placed together therefore, determining the pixels should be suitable for the desired job which requires less resolution, the image files will be smaller. And if it is a work that requires a lot of resolutions, the image file will be large. The resolution of the image on the display will say that the resolution in term of Pixel Per Inch (PPI), which divides the image size as the number of pixels are the resolution of the image displayed on the computer screen. For example, an image with 640 x 480 pixel, 1048 x 960 pixel etc. These 3 RGB values are combined with the red, green and blue the spectral values that are between 0 - 255 in proportion to the concentration. The different spectral values are indicated by the value of the 3 colors that come together in each pixel that resulting in a picture by combining 3 colors in each position of all pixels of the image. The required image encryption is to encryption the 3D chaotic equation at the given default value and perform an Exclusive OR on the RGB color value of each pixel. To produce a new RGB color value mixed with a 3D chaos, the resulting value yields the encryption RGB color value. The image is displayed as a fully encrypted image file, and the image file encryption diagram is shown in Figure 2.

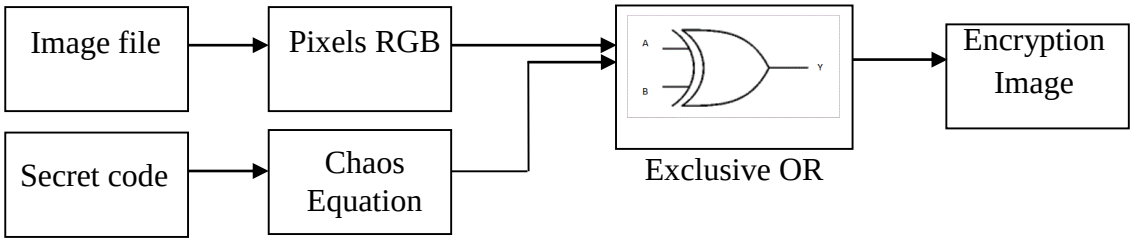


Figure 2 Image file encryption diagram

Let us take the equation to encryption the image file:

$$Original_{image} = [fx(x,y), fy(x,y)]_{R,G,B} \quad (2)$$

$$Encrypted_{image} = Original_{image} \oplus [fx_{Chua}(x,y), fy_{Chua}(x,y)]_{X_0,Y_0,Z_0} \quad (3)$$

Decryption the image files

Decryption takes a similar process to encryption but using a reverse process in which the secret encryption will be used as the starting value of the chaos equation that will give up the solution to do the reverse process to encryption the RGB color of each pixel to restore the original RGB color value to the original image file before it was encrypted, and the image file decryption diagram is shown in Figure 3.

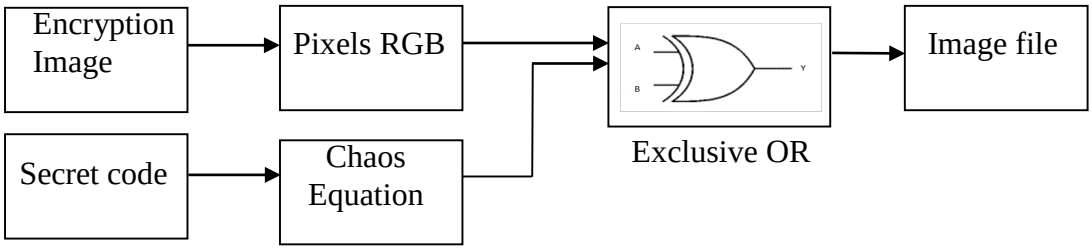


Figure 3 Image file decryption diagram

And the equation to decryption the image file:

$$Decrypted_{image} = Encrypted_{image} \oplus [fx_{Chua}(x,y), fy_{Chua}(x,y)]_{X_0,Y_0,Z_0} \quad (4)$$

Experiment and Discussions

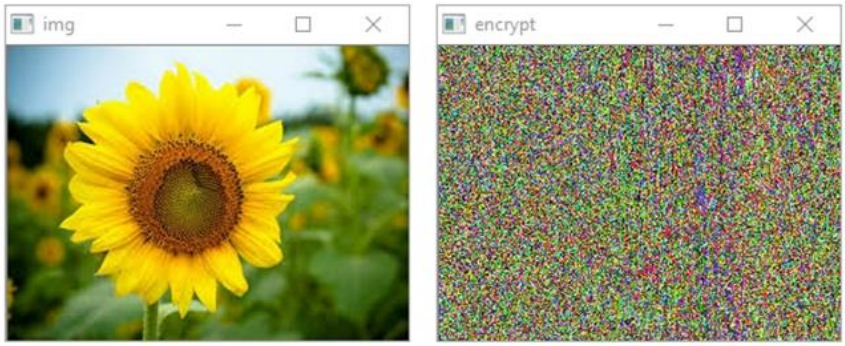
Simulation of encryption and decryption the image files

The mathematical simulation of the chaotic equation of the encryption and decryption the image files in this paper is programmed to compute the image using Python 2.7 program to process the image and display the result (Robert, 2017). The simulation of encryption performs results with Chua equation and decrypts it with the correct secret encryption same as the default

value of encryption with the equation as follows:

$$x_0, y_0, z_0 = [0.111111, 0.111111, 0.111111]$$

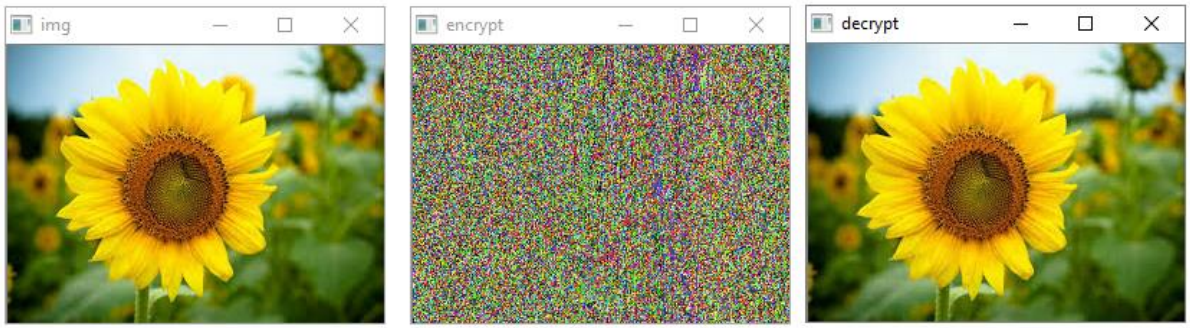
And such encrypted image is shown in Figure 4.



a. original image b. encrypted image

Figure 4 Original image and encrypted image

In the simulation of decryption, the secret encryption is used for encryption is the same secret encryption used decryption that it will get the same picture as the original. And the decrypted image is shown in Figure 5.



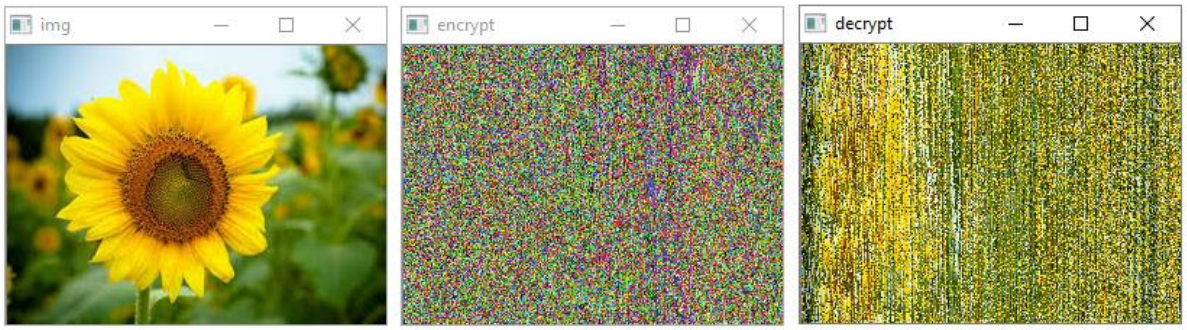
a. original image b. encrypted image c. decrypted image

Figure 5 The encrypted image has been decrypted correctly

If the correct secret encryption for decryption process is not used to encrypt the original image file, the decrypted image will be invalid. Although the secret encryption value for decryption is approximately the same and have inconsistent values, even if they are decimal fractions the image files that can be decrypted will have a picture that is not close to the original image at all. In this simulating decryption whose secret encryption does not match the encryption and we use the secret encryption for decryption as follows:

$$x_0, y_0, z_0 = [0.111112, 0.111112, 0.111112]$$

And such decrypted image is shown in Figure 6.



a. original image b. encrypted image c. decrypted image incorrectly

Figure 6 The encrypted image has been decrypted incorrectly

Conclusions

The process of encryption and decryption are the same algorithm and computer program that must be created in order to reverse algorithm only. This is because of this encryption will encryption the number of 3D array RGB color value in pixels equal to the number of pixels of the image to be encryption three sets of data are encryption in one array, which changes the RGB color value for each pixel from the original image file. There is more processes that are performed with the Exclusive OR function, but it also can reverse decryption process if the secret numbers of the encrypted algorithm are known. Therefore, the design algorithm with Chaos and Chua's Equation used in this encryption process is highly secured and has a simple structure with unwrapping difficult encryption

Moreover, we can apply the chaotic equation to the task that requires a random number with a certain pattern and the resulting numbers have unique values as well.

Recommendation

This research developed encryption and decryption with Chaos and Chua's equation. But it doesn't compare to Chaos encryption with other equations. This may require additional research to compare the efficiency of encryption and decryption to see which equation works best. This may be done with a decryption program to test how well the file is secured. This will give you the best combination of encrypting and decrypting the file.

References

Pitikhet Suksaksa (2007). *Complete research report on "Smart communication and Control Systems for Robotic"*, Thailand Research Fund office.

Klomkarn, K., and P. Sooraksa, *Further investigation on trajectory of chaotic guiding signals for robotic systems*, IEEE Symposium on Communications and Information Technology, vol. 2, Oct 26-29, 2004, pp. 1166-1170.

Joseph Howse, Prateek Joshi, and Michael Beyeler (2016). **"**Open CV: Computer Vision Projects with Python"**.**

Kenneth Dawson-Howe (2014). *"A Practical Introduction to COMPUTER VISION WITH OPEN CV"*.

Robert Laganiere (2017). **"***OpenCV3 Computer Vision Application Programming".*