CHAOS-BASED IMAGE ENCRYPTION SYSTEM UTILIZING ROSSLER ATTRACTOR WITH FUZZY LOGIC

ORLAND DELFINO TUBOLA, JEREMEY PAUL HERRERA

Abstract- The chaos-based cryptographic algorithm offers new ways to develop efficient multimedia encryption schemes which have been motivated by the chaotic properties. The proposed image encryption system uses a Rossler Attractor map which has 3 initial values x, y and z, and 3 parameter values, a, b and c. In addition to this, a fuzzy logic algorithm is used to expand the length of the encryption key through a divisibility rule in order to increase the level of security of the image encryption system. The new encryption key is used as one of the initial values of the Rossler Attractor map to create a set of non-linear values. These set of values are then used in an exclusive operation together with the RGB values of the image. The experimental result of the study involves the use of statistical and security analyses and the proposed image encryption system have been successful in hiding the statistical data of the image and in producing a pure cipher image. Thus, the study has been able to develop a new and improved way of securing an image by using encryption with the help of a fuzzy logic algorithm.

Keywords*:* divisibility rule, chaos system, Rossler Attractor map, image encryption

1. INTRODUCTION

Nowadays, copying and distributing the work of other people can be seen often in the internet because of the fast growing information technology industry and the development of new programs to hack through system domains and computers. In order to prevent data loss and plagiarism, securing the data must be performed with the use of encryption. Since most of the information that can be seen in the internet environment is in the form of an image, an image encryption system is the most practical to study.

With regards to image encryption, the study of chaos systems is often used because of its many similarities with an image encryption process. The chaos systems are non-linear bodies that are sensitive and dependent to their initial conditions. When the initial conditions are changed, the output values will also change dramatically. This property of a chaos system can be applied in an image encryption process wherein the encryption keys entered by the user can be used as the initial conditions of the chaos system.

The main point of an image encryption process is to prevent unauthorized individuals from obtaining the original image. And only individuals who knows the correct encryption key have the right to obtain the original image. And when a wrong key is used in the image encryption system, only a pure noise image should be produced.

Artificial intelligence can be used in addition to an image encryption system in order to eliminate the weaknesses of the system. To determine the level of security and the strength and weaknesses of an image encryption system, different statistical and security analyses can be performed such as histogram analysis, entropy analysis and correlation coefficient analysis.

2. THE PROPOSED ENCRYPTION SCHEME

This study aims to create a chaos-based image encryption system utilizing Rossler Attractor map with Fuzzy Logic. The level of security of the image encryption process will be the main focus in this study. The main problem of most image encryption schemes with respect to security is the key space and since an encryption key is the part that mostly contribute to this problem, because of its limited character space, a fuzzy logic algorithm is used to implement a set of rules for expanding the length of the encryption key. The encryption key used in this study can only accept numeric character that ranges from 0 to 9. The fuzzy logic rule aims to transform the encryption key into a new set of characters by multiplying the encryption key with a set of fixed numbers that are dependent on the divisibility of the encryption key.

The Fuzzy Logic Divisibility Rules

- If the encryption key is divisible by 10 then multiply it by the length of the encryption key 10 times.
- If the encryption key is divisible by 9 then multiply it by the length of the encryption key 9 times.
- If the encryption key is divisible by 8 then multiply it by the length of the encryption key 8 times.
- If the encryption key is divisible by 7 then multiply it by the length of the encryption key 7 times.
- If the encryption key is divisible by 6 then multiply it by the length of the encryption key 6 times.
- If the encryption key is divisible by 5 then multiply it by the length of the encryption key 5 times.
- If the encryption key is divisible by 4 then multiply it by the length of the encryption key 4 times.
- If the encryption key is divisible by 3 then multiply it by the length of the encryption key 3 times.
- If the encryption key is divisible by 2 then multiply it by the length of the encryption key 2 times.
- If the encryption key is a prime number then multiply it by the length of the encryption key.

After the fuzzy logic process, the expanded encryption key is used as one of the initial conditions of the Rossler Attractor map. The Rossler Attractor map is a three dimensional non-linear system that uses x, y and z as its initial values and a, b and c as its parameters.

The Rossler Attractor can be described using the following equations:

$$\frac{dx}{dt} = -y - z \qquad (1)$$

$$\frac{dy}{dt} = x + ay \qquad (2)$$

$$\frac{dz}{dr} = b + z\,(x - c) \qquad (3)$$

In this study, the initial values x, y and z are all set to 0.1 while parameter a is set to 0.2 and parameter c is set at 5.7. Parameter b of the Rossler Attractor map will have a value of 0.1 concatenated with a single digit value that comes from the expanded encryption key. A Simulink model was constructed in order to prove the functionality of the initial conditions.

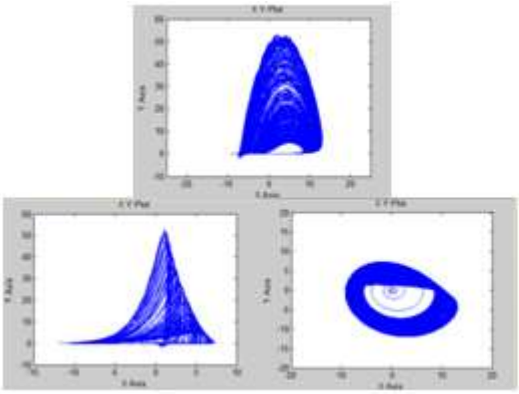


Fig. 1 Plot of the X and Y, Y and Z and X and Z axes of the Simulink Model of the Rossler Attractor map at initial conditions of a = 0.2, b = 0.1, c = 5.7, x =0.1, y = 0.1 and z = 0.1.

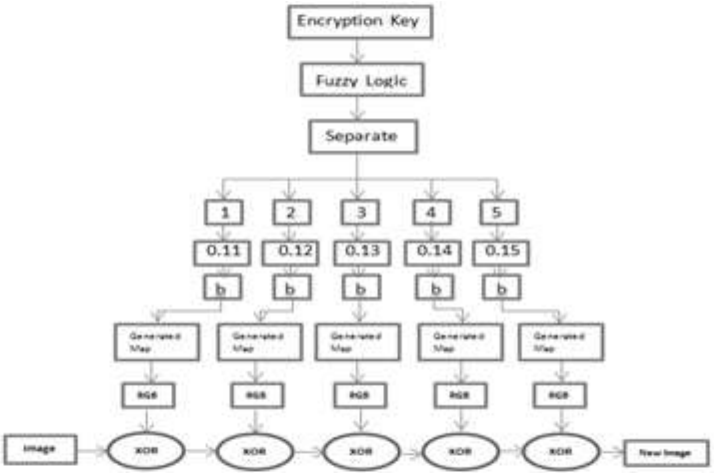


Fig. 2 Procedure of the proposed chaos-based image encryption system

Fig.2 shows an example of the main process of the proposed chaos-based image encryption system wherein the topmost box is the encryption key entered by the user, the lower left box is the image to be encrypted, the middle boxes represent the Rossler Attractor map and the exclusive or functions and the lower right box is the new image produced by the proposed chaos-based image encryption system.

The Proposed Chaos-Based Image Encryption System Procedure

1. Enter the image that needs to be encrypted and the desired numeric encryption key.
2. Implement the fuzzy logic divisibility rule to expand the length of the encryption key.
3. Separate the digits of the newly expanded encryption key.
4. Concatenate a single digit in procedure number 4 to a 0.1 value.
5. Use the values in procedure number 5 as parameter b and generate the Rossler Attractor map.
6. Create a similar-sized matrix for each dimension of the image entered in procedure number 1.

7. Put the values generated by the Rossler Attractor map into the matrices.
8. Keep generating values from the Rossler Attractor map until all the matrices are filled with values.
9. Use an exclusive or (XOR) function between each dimensions of the image and the matrices prepared in procedure number 8.
10. Repeat procedure numbers 4 to 9 for the next single digit number in procedure number 3.

3. EXPERIMENTAL RESULTS

The Baboon, F16 and House images are used to test the functionality of the image encryption system.

Table 1 Encrypted and decrypted test images

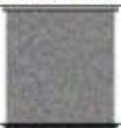
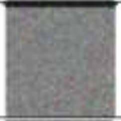
Image Name	Original Image	Encrypted Image; key 325801019	Decrypted Image; correct key 325801019
Baboon			
F16			
House			

Table 1 shows how the proposed image encryption system had encrypted and decrypted the test images. When the test images are all encrypted with the same encryption key 325801019, it produced a noise like image that does not contain any trace of the original image and when the encrypted test images are decrypted using the same encryption key 325801019, the original test images were completely recovered.

Security Analysis

Key Space Analysis

The key space is the set of all possible combinations of characters to produce an encryption key. In this study, the encryption key, which is composed of numeric characters that range from 0 to 9, is limited into a 10^n possible encryption keys. But since the length of the proposed image encryption system's encryption key is indefinite, the key space can be defined as 10^{∞} or an infinite combination of numeric characters.

Key Sensitivity Analysis

The key sensitivity analysis is the study that involves how the image encryption system handles wrong encryption keys, especially those that have slight difference from the correct encryption key.

Table 2 Decrypted test images with wrong decryption keys

Image Name	Decrypted Image; wrong key 325801018 (w/o Fuzzy Logic)	Decrypted Image; wrong key 325801918 (w/ Fuzzy Logic)
Baboon		
F16		
House		

Table 2 shows how the proposed image encryption system had decrypted the encrypted image using different kinds of image encryption system and an encryption key that has slight difference from the correct encryption key. When the encrypted image was decrypted using the image encryption system that does not involve the fuzzy logic rules, it produced an image that contains some traces of the original image while when the encrypted image was decrypted the image encryption system that uses the fuzzy logic rules, it still produces a pure noise image.

Statistical Analysis

Image Histogram Analysis

The Histogram analysis is a diagram consisting of rectangles that represent the frequency of the tone of each pixel values of an image. An effective image encryption system is expected to produce a flat distributed histogram of the encrypted image so that no statistical data can be seen through the image.

Table 3 Image Histogram Analysis of the original, encrypted and decrypted Baboon images

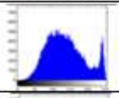
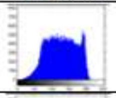
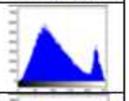
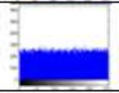
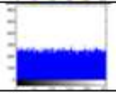
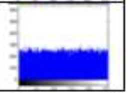
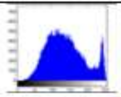
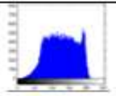
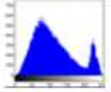
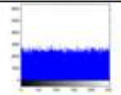
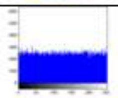
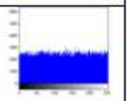
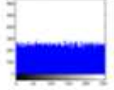
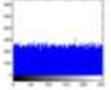
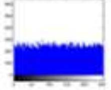
Image Name	Red Dimension	Green Dimension	Blue Dimension
Original Image			
Encrypted Image;key 325801019			
Decrypted Image; correct key 325801019			
Decrypted Image; wrong key 325801018 (w/o Fuzzy Logic)			
Decrypted Image; wrong key 325801018 (w/ Fuzzy Logic)			

Table 4 Histogram analysis of the original, encrypted and decrypted F16 images

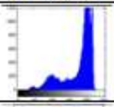
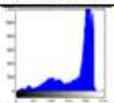
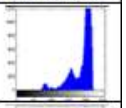
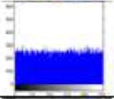
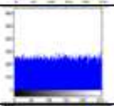
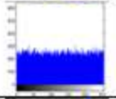
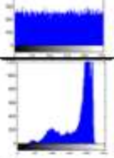
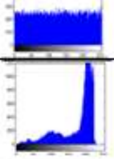
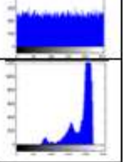
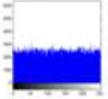
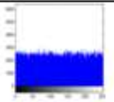
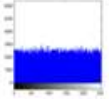
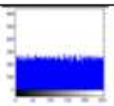
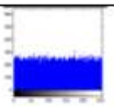
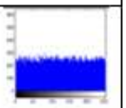
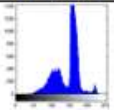
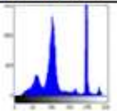
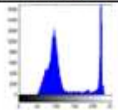
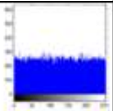
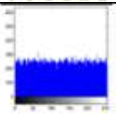
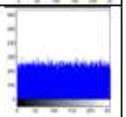
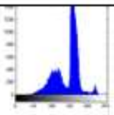
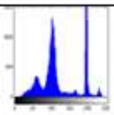
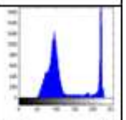
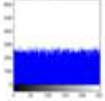
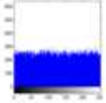
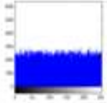
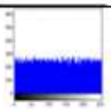
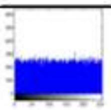
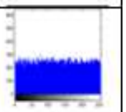
Image Name	Red Dimension	Green Dimension	Blue Dimension
Original Image			
Encrypted Image; key 325801019			
Decrypted Image; correct key 325801019			
Decrypted Image; wrong key 325801018 (w/o Fuzzy Logic)			
Decrypted Image; wrong key 325801018 (w/ Fuzzy Logic)			

Table 5 Histogram analysis of the original, encrypted, decrypted House images

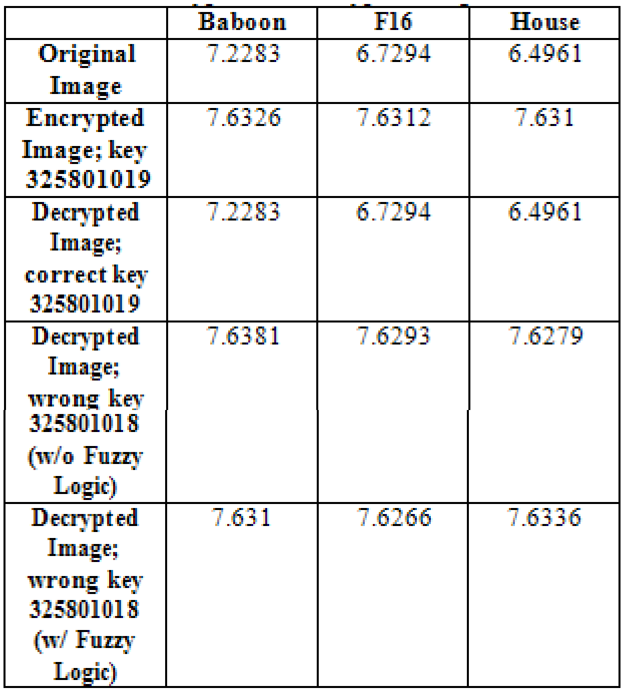
Image Name	Red Dimension	Green Dimension	Blue Dimension
Original Image			
Encrypted Image; key 325801019			
Decrypted Image; correct key 325801019			
Decrypted Image; wrong key 325801018 (w/o Fuzzy Logic)			
Decrypted Image; wrong key 325801018 (w/ Fuzzy Logic)			

Tables 3, 4 and 5 show the histogram changes of the images. It can be seen in the tables that as the test images are encrypted, their histograms change from randomly distributed histograms into flat distributed histograms while when these encrypted test images are decrypted using the correct encryption key, their histograms returned to their original histograms. But when the encrypted test images are decrypted using wrong encryption keys and without fuzzy logic, their histograms are still flat distributed histograms.

Information Entropy Analysis

The information entropy is a statistical value that represents the randomness of the texture of an image. An effective image encryption system is expected to produce an encrypted image that has a minimum value of 8 information entropy value to ensure the randomness of the whole image.

Table 6 Information entropy values of original, encrypted and decrypted images



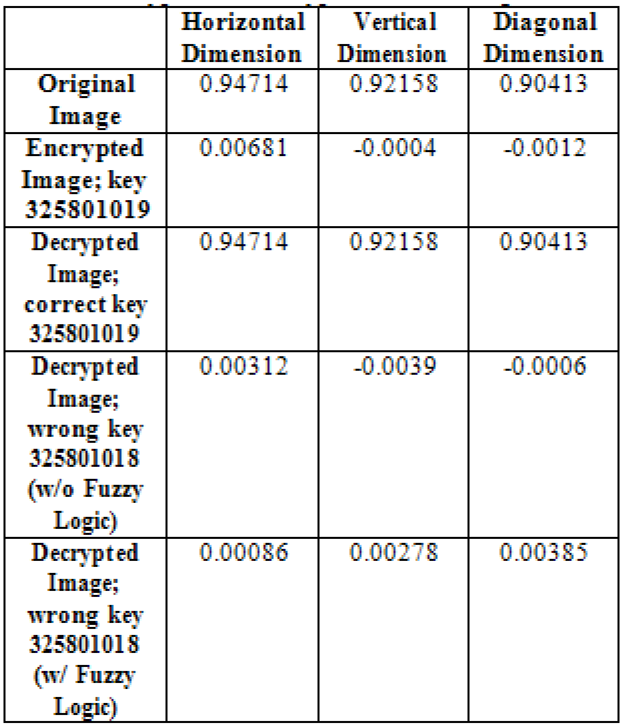
	Baboon	F16	House
Original Image	7.2283	6.7294	6.4961
Encrypted Image; key 325801019	7.6326	7.6312	7.631
Decrypted Image; correct key 325801019	7.2283	6.7294	6.4961
Decrypted Image; wrong key 325801018 (w/o Fuzzy Logic)	7.6381	7.6293	7.6279
Decrypted Image; wrong key 325801018 (w/ Fuzzy Logic)	7.631	7.6266	7.6336

Tables 6 shows the new information entropy of the test images, after the encryption process, increases above 7.6 values while when the encrypted test image is decrypted using the correct encryption key their information entropy returned back into their original values. And when decrypting the encrypted test images using wrong encryption keys, the information entropy values still remain at a high value.

Correlation Coefficient Analysis

The correlation coefficient analysis determines the strength of relationship between two variables. An effective image encryption system is expected to produce an almost zero correlation coefficient value of the encrypted image, to hide the relationship of the variables of the encrypted image.

Table 7 Correlation coefficient values of the original, encrypted and decrypted baboon images



	Horizontal Dimension	Vertical Dimension	Diagonal Dimension
Original Image	0.94714	0.92158	0.90413
Encrypted Image; key 325801019	0.00681	-0.0004	-0.0012
Decrypted Image; correct key 325801019	0.94714	0.92158	0.90413
Decrypted Image; wrong key 325801018 (w/o Fuzzy Logic)	0.00312	-0.0039	-0.0006
Decrypted Image; wrong key 325801018 (w/ Fuzzy Logic)	0.00086	0.00278	0.00385

Table 8 Correlation coefficient plots of the original, encrypted and decrypted baboon images

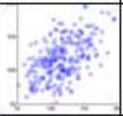
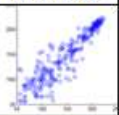
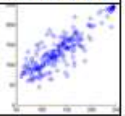
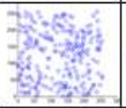
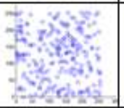
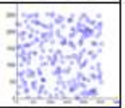
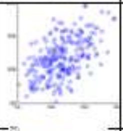
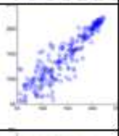
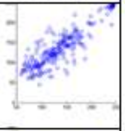
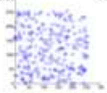
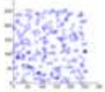
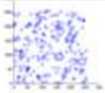
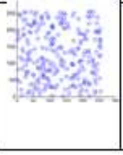
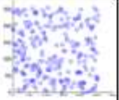
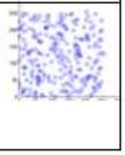
	Horizontal Dimension	Vertical Dimension	Diagonal Dimension
Original Image			
Encrypted Image; key 325801019			
Decrypted Image; correct key 325801019			
Decrypted Image; wrong key 325801018 (w/o Fuzzy Logic)			
Decrypted Image; wrong key 325801018 (w/ Fuzzy Logic)			

Table 9 Correlation coefficient analysis of the original, encrypted and decrypted F16 images

	Horizontal Dimension	Vertical Dimension	Diagonal Dimension
Original Image	0.93852	0.92519	0.87526
Encrypted Image; key 325801019	0.01251	0.00308	-0.0052
Decrypted Image; correctkey 325801019	0.93852	0.92519	0.87526
Decrypted Image; wrong key 325801018 (w/o Fuzzy Logic)	0.01119	-0.0048	-0.0036
Decrypted Image; wrong key 325801018 (w/ Fuzzy Logic)	0.00417	0.00222	0.00061

10 Correlation coefficient plots of the original, encrypted and decrypted F16 images

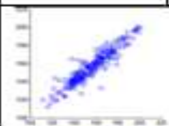
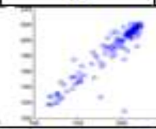
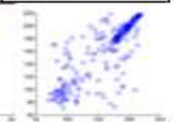
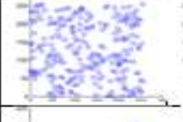
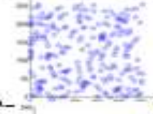
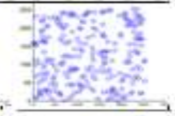
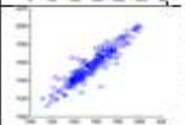
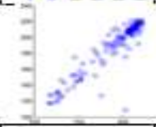
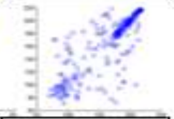
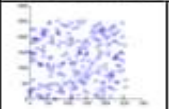
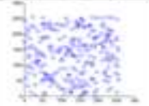
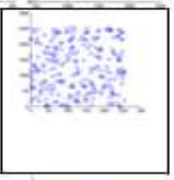
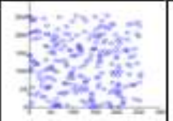
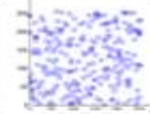
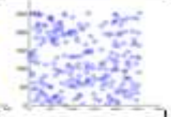
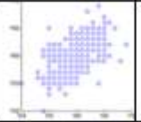
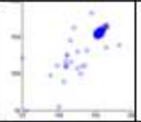
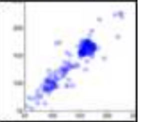
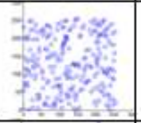
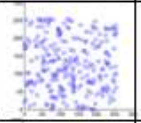
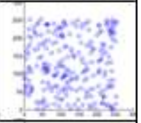
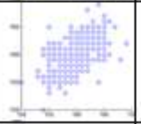
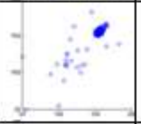
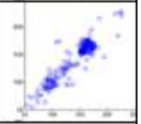
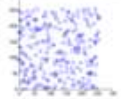
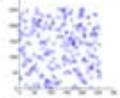
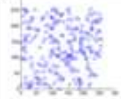
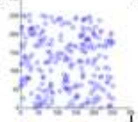
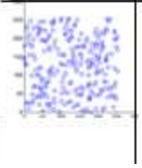
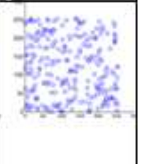
	Horizontal Dimension	Vertical Dimension	Diagonal Dimension
Original Image			
Encrypted Image; key 325801019			
Decrypted Image; correct key 325801019			
Decrypted Image; wrong key 325801018 (w/o Fuzzy Logic)			
Decrypted Image; wrong key 325801018 (w/ Fuzzy Logic)			

Table 11 Correlation coefficient value of the original, encrypted and decrypted house images

	Horizontal Dimension	Vertical Dimension	Diagonal Dimension
Original Image	0.96703	0.93527	0.91264
Encrypted Image; key 325801019	0.00555	-0.0001	-0.0034
Decrypted Image; correctkey 325801019	0.96703	0.93527	0.91264
Decrypted Image; wrong key 325801018 (w/o Fuzzy Logic)	0.00331	0.00327	0.00509
Decrypted Image; wrong key 325801018 (w/ Fuzzy	0.00130	0.00529	-0.0101

Table 12 Correlation coefficient plots of the original, encrypted and decrypted F16 images

	Horizontal Dimension	Vertical Dimension	Diagonal Dimension
Original Image			
Encrypted Image; key 325801019			
Decrypted Image; correct key 325801019			
Decrypted Image; wrong key 325801018 (w/o Fuzzy Logic)			
Decrypted Image; wrong key 325801018 (with Fuzzy Logic)			

Tables 7, 8, 9, 10, 11 and 12 show that after the original images have been encrypted, their correlation values have been decreased to a very small value and their plots have become scattered. The nearer the value to zero, the weaker the relationship of the set of values and the lesser the amount of information that can be traced on the encrypted image and the distances between their plots represent how the encrypted images have weak relationships. In decrypting the encrypted image with the use of the correct encryption key, it can be seen in the table that the correlation coefficient values and plots are returned to their original while decrypting the encrypted images using wrong decryption keys, the correlation values and plots still represent a very weak correlation coefficient.

4. CONCLUSION

Based on the results of the statistical and security analyses done on the proposed system it is safe to conclude that utilizing Rossler Attractor map with fuzzy logic in image encryption offers a high level of data security. The proposed image encryption system has been able to successfully hide the statistical data of the images by having a high entropy values of more than 7.6, low correlation coefficient values of 0.003 and flatly distributed histograms. In addition to these statistical data, attackers could not easily obtain the correct encryption key because the proposed image encryption system uses 2^{∞} possible character combinations for the encryption key which makes the key space of the proposed image encryption system theoretically infinite.

5. REFERENCES

[1] Bellare, M., & Rogaway, P. (2005). *Introduction to Modern Cryptography.* California: Mihir Bellare and Phillip Rogaway.

[2] Davies, B. (2004). *Exploring Chaos: Theory and Experiment.* Colorado: Westview Press.

[3] Farazmand, A. (2003). Chaos and Transformation Theories: A Theoretical Analysis with Implications for Organization Theory and Public Management. 372.

[4] Gao, H. Z. (2005). *A New Chaotic Algorithm for Image Encryption.* Chaos, Solitons and Fractals.

[5] Hameed, S. R. (2011). Modified Advanced Encryption Standard for Text and Images.

[6] Han, W. X. (2003). *A New Image Encryption Algorithm Based on Chaos System.* Changsha, China: International Conference on RoboticsJntelligent Systems and Signal Processing.

[7] Jakimoski, G. a. (2001). Chaos and Cryptography: Block Encryption Ciphers. Chaos and Cryptography: Block Encryption Ciphers.

[8] L., K. (2001). Chaos and Cryptography:a brief Overview. *IEEE Circuits and Systems Magazine* , pp. 6-21.

[9] Mao, Y. C. (2003). *A Novel Fast Image Encryption Scheme Based on 3D Chaotic Baker Maps.* Hongkong, China: World Scientific Publishing Company.

[10] Mirasso, C. R. (2002). *Introduction to the Feature Section on Optical Chaos.* IEEE JOURNAL OF QUANTUM ELECTRONICS.

[11] Mitra, A. R. (2006). A New Image Encryption Approach using Combinational Permutation Techniques.

[12] Murali, H. Y. (2001). *SECURE COMMUNICATION USING A CHAOS BASED SIGNAL ENCRYPTION SCHEME.* Department of Physics, Anna University.

[13] Ozturk, I. a. (2005). *Analysis and Comparison of Image Encryption Algorithms.* Gebze Institute of Technology Computer Eng. Dept.

[14] Pareek, N. K. (2005). *Image encryption using chaotic logistic map.* Rajasthan, India: Image and Vision Computing.

[15] Patel, K. D. (2011). *Image Encryption Using Different Techniques: A Review.* International Journel of Emerging Technology and Advanced Engineering.

[16] Rajasekaran, S., & Pai, G. V. (2003). *Neural Networks, Fuzzy Logic and Genetic Algorithms: Synthesis and Applications.* New Delhi: Prentice-Hall of India Private Limited.

[17] Sivanandam, S., Sumathi, S., & Deepa, S. (2007). *Introduction to Fuzzy Logic Using MATLAB.* New York: Springer-Verlag Berlin Heidelberg.

[18] Uhl, A., & Pommer, A. (2005). *Image and Video Encryption: From Digital Rights Management to Secured Personal Communication.* New York: Springer Science Business Media, Inc.

Department of Computer Engineering, College of Engineering, Polytechnic University of the Philippines