PERFORMANCE ANALYSIS OF SEVERAL CHAOS-BASED IMAGE ENCRYPTION SYSTEMS WITH SIMPLE FUZZY LOGIC

ORLAND DELFINO TUBOLA, JEREMY PAUL HERRERA

Abstract – A performance analysis of chaos-based image encryption system with simple fuzzy logic is proposed in this paper involving several chaotic maps. Some of the chaotic maps known today were used to conclude the image security the system can offer when used in an encryption scheme. Each of their security capabilities was determined to identify which is ideal or not for securing image data. Upon evaluating all the involved chaotic maps, it was hereby realized that using a chaos-based scheme for encrypting images still offers weaker security because it still leaves a recognizable pattern of the original image ciphered. The incorporation of simple fuzzy logic resolved this problem by amplifying the values exhibited by every chaotic map, thus, resulting to ciphered images that have higher level of unpredictability, greater randomness of information content and a more sensitive encryption key as presented in the security analysis conducted by the proponents of this study.

Keywords: performance analysis, chaotic maps, image encryption, fuzzy logic

1. INTRODUCTION

Data, by any means, should be protected from illegal access and misuse by cyber criminals. With this, data security plays an important role in keeping every bits of information safe from hacking and unauthorized intents. There are four kinds of internal security controls that can be enforced in data protection-access, flow, inference and cryptographic controls [1]. These controls regulate operation of the computer system in different areas: access to stored objects such as file, flow of information from one stored object to another, inference of confidential information stored in statistical databases, and encryption of confidential data stored in files or transmitted on communications lines. In this paper, encryption was emphasized as it is used in securing one of the electronic information people usually deal at most – images. In image encryption, image data is transformed in a key-dependent cipher having unpredictable statistical data. Encryption is the process of converting information into an encrypted form, so that it is intelligible only to someone who knows its key [2].

On the early 1950's Claude Shannon (1916-2001) mentioned that the basic stretch and fold mechanism of chaos can be used in cryptology [3] specifically in encryption. Since chaotic dynamics is sensitive to initial conditions, even a small difference on the key will end up to a wildly different outcome. A chaotic system is a non-linear, dynamic system that has sensitive dependence on initial conditions, mixing and dense periodic points [4]. There are several chaotic maps known today. Upon iterating these chaotic maps, a secret key cryptosystem can be produced that has sensitive parameters and initial points and randomness of sequences. This cryptosystems are effective for securing image data by means of higher degree of randomization that is used in the process. Therefore, image encryption approach based on chaotic maps is useful, efficient and highly secure.

2. THE PROPOSED ENCRYPTION SCHEME

2.1 Chaotic Maps

The idea that chaos theory could be used to generate encryption keys is not necessarily new, but less likely to be used in such a scheme. In this analysis, several chaotic maps were injected in a uniform encryption system to test its performance with regards to ciphering plain images. Each map has its own parameters and different values for their variables that constitute a lot with its ciphering capability.

Chaotic maps can be either one-dimensional, two dimensional or more with either complex or real variables. In this paper, each chaotic map differs obviously from their X and Y-components. It is known that the higher the number of constants the map has, the larger its key space is and the more complex the equations are, the better its encryption capability.

Table 1. Equations of Several Chaotic Maps

Chaos Map	Formulas
Burgers Map (BM) [6]	$x_{n+1} = (1 - \nu)x_n - y_n^2$ $y_{n+1} = (1 + \mu)y_n + x_n y_n$
Chirikov Standard Map (CSM) [21]	$p_{t+1} = p_n + K\sin(\chi_n)$ $\chi_{t+1} = p_t + \chi_t$
Circle Map (CM) [23]	$f(x) = x + \Omega + ksin^2 x$
Complex Quadratic Map (CQM) [21]	$z_{n+1} = c + z_n^2$
Cross Chaotic Map (CCM) [23]	$x_{i+1} = 1 - \mu y_i^2$ $y_{i+1} = \cos(k\cos^{-1} x_i)$
Duffing Map (DM) [2]	$x_{n+1} = y_n$ $y_{n+1} = bx_n + ay_n - y_n^2$
Gingerbread Man Map (GIMM) [16]	$\Phi 1(\mathrm{X}) = 1 - x_2 + \lvert x_1 \rvert$ $\Phi 2(X) = x_1$
Gumowski Mira Map (GUMM) [14]	$x_{n+1} = y_{n+1} + \mathrm{a}(1 - 0.05y_n^2)y_n + f(x_n)$ $y_{n+1} = -x_n + f(x_{n+1})$
Henon Map (HM) [2]	$x_{i+1} = 1 - \ \alpha x_n^2 + y_i$ $y_{i+1} = bx_i$
Ikeda Map (IM) [11]	$x_{n+1} = 1 + u[x_n \cos t_n - y_n \sin t_n]$ $y_{n+1} = u[x_n \sin t_n + y_n \cos t_n]$
Kaplan Yorke Map (KYM) [2]	$x_{n+1} = a_n / b$ $a_{n+1} = a_0 + 2a_n^2(mod\ b)$ $y_{n+1} = \alpha y_n + \cos(4\pi x_n)$
Lozi Map (LM) [22]	$x_{n+1} = 1 + y_n - a\lvert x_n \rvert$ $y_{n+1} = bx_n$
Rabinovich-Fabrikant Equation (RFE) [12]	$x_{n+1} = y(z - 1 + x^2) + ax$ $y_{n+1} = x(3z + 1 - x^2)ay$ $z_{n+1} = -2z(b + xy)$
Tinkerbell Map (TM) [9]	$y_{n+1} = y_n^2 - \theta_n^2 + \alpha y_n + \beta\theta_n$ $\theta_{n+1} = 2y_n\theta_n + \gamma y_n + \delta\theta_n$
Van Der Pol Oscillator (VDPO) [13]	$\dot{\mathrm{x}}_1 = x_2(x_3 - 1 + x_1^2) + ax_1$ $\dot{\mathrm{x}}_2 = x_1(3x_3 + 1 - x_1^2) + ax_2$ $\dot{\mathrm{x}}_3 = -2x_3(b + x_1 x_2)$

Table 1 shows the different equations of several chaotic maps involved in this paper. To test its security features, derived mathematical models are created from each map and were set as a random number generator one at a time. Security analysis was conducted in every chaos-based image encryption systems tested and was further discussed in Section 3.2.

2.3 Embedding Fuzzy Logic Algorithm

Fuzzy logic can model nonlinear functions of arbitrary complexity [5]. It can provide a rich and meaningful addition to the chaos-based scheme used, thus, fuzzy logic was able to create a system that can aid the encryption process to its ideal function. Fuzzy logic rules define the behaviour of the encryption system. The rules were made exclusively for the encryption key amplification and were applied to several chaotic maps. Since the random values exhibited by most Chaos model, is small and produces weak security. Adding fuzzy logic as a key intensifier would be a great way of improving the current chaos-based encryption scheme.

Fuzzy logic inference system was used to increase the values fed by every chaotic map model to the scheme. In doing so, the large key space was retained but the keys fed one at a time was differed and more importantly, it was enlarged, thus, adding security to the encryption scheme. In each fuzzy inference system, both input and output have 10 uniform membership functions.

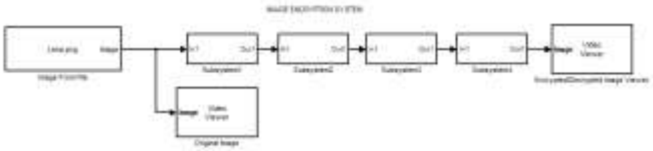


Figure 1 Image Encryption System

Figure 1 serves as the final chaos-based image encryption system with fuzzy logic that was used by the chaotic maps involved in this paper.

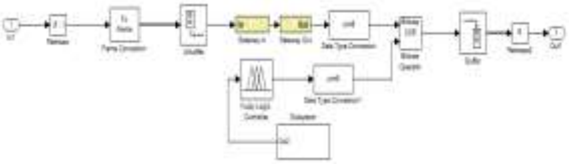


Figure 2 Encryption Subsystem with Fuzzy Logic Controller

Figure 2 illustrates the encryption subsystem with its added fuzzy logic controller. The controller calls the generic fuzzy inference system. Simultaneously, the output from the model's subsystem was set as the input of the controller. It regulates new keys that will be bit-wised XOR with the corresponding values of image data.

3. EXPERITIMENTAL RESULTS

Upon testing each chaotic map presented in Table 1 as used in the chaos-based image encryption scheme with simple fuzzy logic, experimental results were recorded and analysed. Two images were used namely Lena and Photographer images and their corresponding experimental results for each map are presented in Tables 2.1 and 2.2 for Lena, and Tables 3.1 and 3.2 for Photographer.

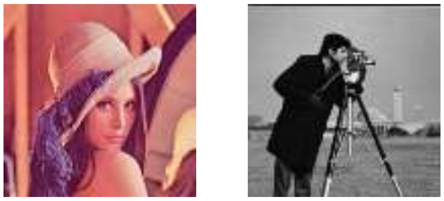


Figure 3 Original Images of Lena and Photographer

3.1 Security Analysis

Many ciphers have been successfully analysed with the help of security analysis. Several statistical attacks have been formulated to test their encryption ability. To substantiate the robustness of the proposed encryption scheme and the idealness of several chaotic maps involved, statistical analysis was done such as getting the histogram and testing encryption key sensitivity of every chaotic map. Also, finding entropy and correlation coefficients of the experimental results were conducted.

3.1.1 Histogram Analysis

Histograms are used to estimate how the values of a variable are distributed across a certain range [7]. It can graphically summarize and display the distribution and variation of the pixel intensity values. As for its significance, it can give knowledge about the system that will act as a guide to improve its security.

3.1.2 Correlation Coefficient Analysis

To test the strength of every chaos-based image encryption scheme with regards to its strength and direction of linear association between two variables, correlation coefficient analysis [8] was conducted. The correlation coefficient is a number between -1 and 1. It is known that having zero or near zero coefficient is ideal for an image encryption scheme.

3.1.3 Information Entropy Analysis

Entropy is the measure of unpredictability of information content. An ideal encrypted image should have entropy value 8 but if an encrypted image has entropy value less than 8 then there must be a certain degree of predictability, which threatens its security [18]. As for its essence, the higher the entropy values of an encrypted image, the better the security it can offer for image data.

The histogram, correlation coefficient and entropy values achieved from every experimental result are presented in Tables 2.1 and 2.2 for Lena and 3.1 and 3.2 for Photographer.

Table 2.1 Encrypted Images of Lena and their corresponding Histograms, Information Entropy Values and Correlation Coefficient Plot

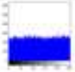
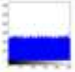
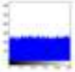
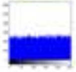
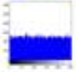
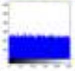
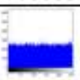
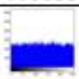
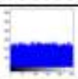
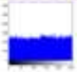
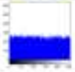
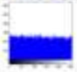
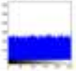
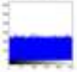
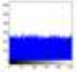
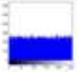
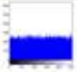
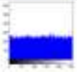
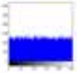
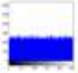
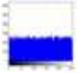
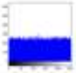
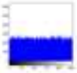
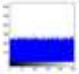
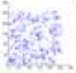
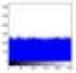
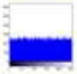
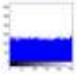
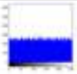
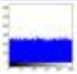
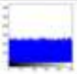
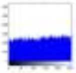
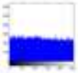
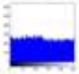
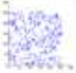
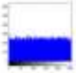
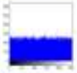
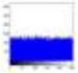
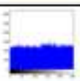
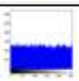
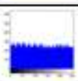
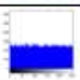
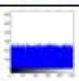
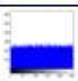
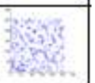
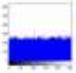
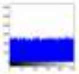
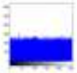
Chaos Map	Encrypted Images							
	Image	Histogram			Entropy	Correlation Coefficient		
		Red	Green	Blue		Horizontal	Vertical	Diagonal
BM					7.6303			
CSM					7.629			
CM					7.6238			
CQM					7.631			
CCM					7.6312			
DM					7.6289			
GIMM					7.6277			
GUMM					7.6273			
HM					7.6272			
IM					7.6313			
KYM					7.6274			
LM					7.6301			
RFE					7.6237			
					7.6259			
VDPO					7.633			

Table 2.2 Decrypted Images of Lena and their corresponding Histograms, Information Entropy Values and Correlation Coefficient Plot

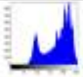
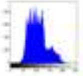
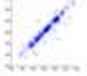
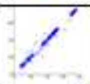
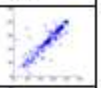
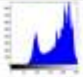
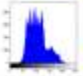
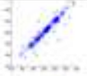
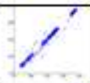
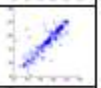
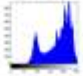
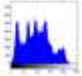
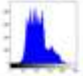
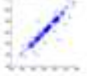
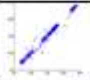
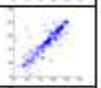
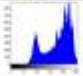
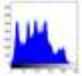
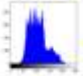
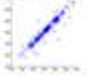
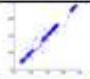
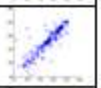
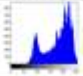
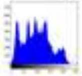
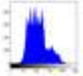
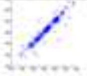
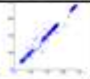
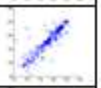
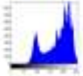
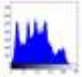
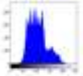
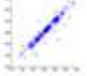
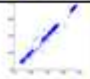
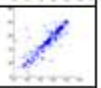
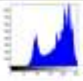
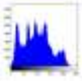
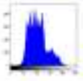
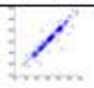
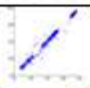
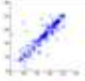
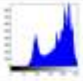
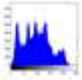
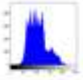
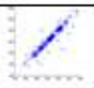
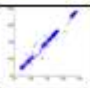
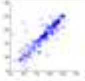
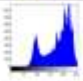
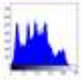
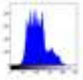
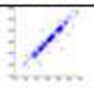
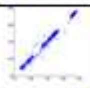
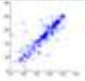
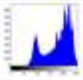
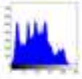
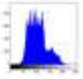
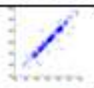
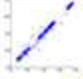
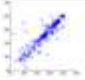
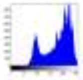
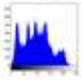
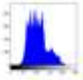
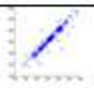
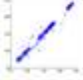
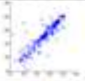
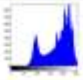
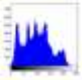
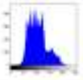
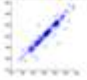
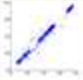
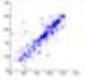
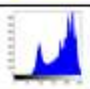
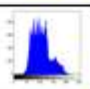
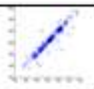
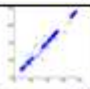
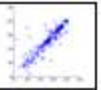
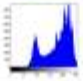
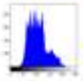
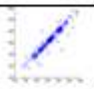
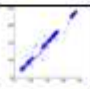
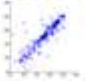
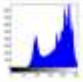
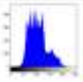
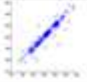
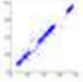
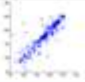
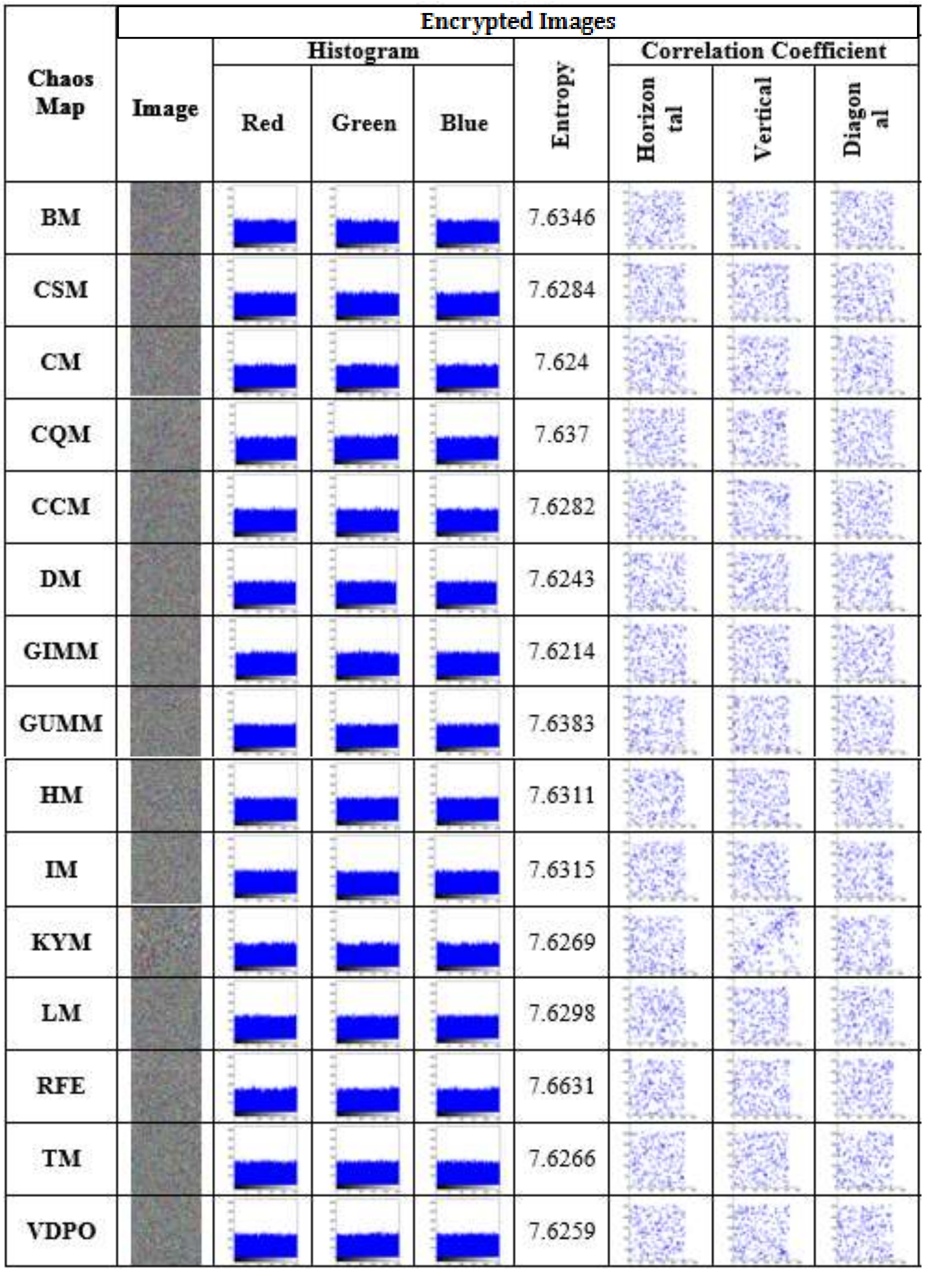
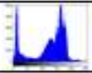
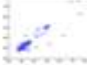
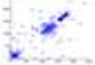
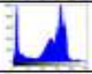
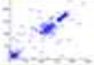
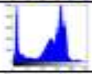
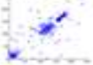
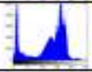
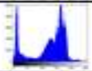
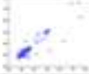
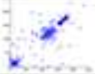
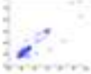
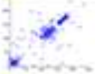
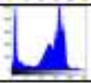
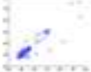
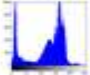
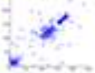
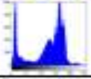
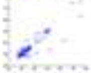
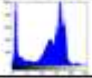
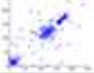
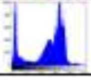
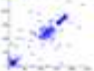
Chaos Map	Decrypted Images							
	Image	Histogram			Entropy	Correlation Coefficient		
		Red	Green	Blue		Horizontal	Vertical	Diagonal
BM					7.4468			
CSM					7.4468			
CM					7.4468			
CQM					7.4468			
CCM					7.4468			
DM					7.4468			
GIMM					7.4468			
GUMM					7.4468			
HM					7.4468			
IM					7.4468			
KYM					7.4468			
LM					7.4468			
RFE					7.4468			
					7.4468			
VDPO					7.4468			

Table 3.1 Encrypted Images of Photographer and their corresponding Histograms, Information Entropy Values and Correlation Coefficient Plot



Chaos Map	Encrypted Images							
	Image	Histogram			Entropy	Correlation Coefficient		
		Red	Green	Blue		Horizontal	Vertical	Diagonal
BM					7.6346			
CSM					7.6284			
CM					7.624			
CQM					7.637			
CCM					7.6282			
DM					7.6243			
GIMM					7.6214			
GUMM					7.6383			
HM					7.6311			
IM					7.6315			
KYM					7.6269			
LM					7.6298			
RFE					7.6631			
TM					7.6266			
VDPO					7.6259			

Table 3.1 Decrypted Images of Photographer and their corresponding Histograms, Information Entropy Values and Correlation Coefficient Plot

Chaos Map	Decrypted Images					
	Image	Histogram	Entropy	Correlation Coefficient		
				Horizontal	Vertical	Diagonal
BM			7.1468			
CSM			7.1468			
CM			7.1468			
CQM			7.1468			
CCM			7.1468			
DM			7.1468			
GIMM			7.1468			
GUMM			7.1468			
HM			7.1468			
IM			7.1468			
KYM			7.1468			
LM			7.1468			
RFE			7.1468			
TM			7.1468			
VDPO			7.1468			

Tables 2.1 and 2.2 for Lena, and 3.1 and 3.2 for Photographer illustrate that each of the different chaos-based image encryption systems produces a distinct way of completely encrypting an image, flattening of histograms,

increasing information entropy values and spreading out correlation coefficient plots which are all good characteristic of an effective image encryption. Moreover, the different chaos-based image encryption systems are capable of decrypting the image successfully.

3.1.4 Key Sensitivity Analysis

An ideal image encryption procedure should be sensitive with respect to the secret key, for example, the change of a single bit in the secret key should produce a completely different encrypted or decrypted image.

Table 4. Decrypted Images using wrong encryption key

Chaos Map	Lena	Photo-grapher	Chaos Map	Lena	Photo-grapher
BM			HM		
CSM			IM		
CM			KYM		
CQM			LM		
CCM			RFE		
DM			TM		
GIMM			VDPO		
GUMM					

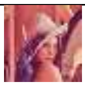
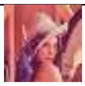
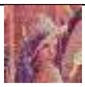
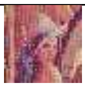
Table 4 illustrates a decryption process of the 15 different chaos-based image encryption systems using correct encryption key that has its single last bit changed to another value. This proves that any wrong encryption key, regardless that some of its bits are correct cannot get authorization over the image.

3.1.5 Non-Fuzzy Vs Fuzzy

Moving on, to prove that adding fuzzy logic to the encryption scheme really adds security to the system, security analysis was conducted comparing the decrypted images of the chaos-based image encryption scheme with fuzzy logic and without fuzzy logic. By doing so, the proponents were able to distinguish the development of the system upon incorporating fuzzy logic to the scheme.

Table 5 below illustrates that compared to the chaos-based image encryption system with fuzzy logic, some chaotic maps needs fuzzy logic for improvement of their security and some chaotic maps cannot encrypt an image without the fuzzy logic algorithm. Overall, the fuzzy logic has given all of the 15 different chaos-based image encryption systems a better and higher security.

Table 5. Encrypted Images of Lena and Photographer and their corresponding information entropy values (w/o Fuzzy Logic)

Chaos Map	**Lena**		**Photographer**	
	Image	**Entropy**	**Image**	**Entropy**
BM		7.3107		7.1563
CSM		7.3403		7.1564
CM		7.3054		7.1231
CQM		2.5779		2.5779
CCM		7.3122		7.1655
DM		7.3405		7.1512
GIMM		7.3281		7.184
GUMM		7.4915		7.1474
HM		7.4468		7.1469
IM		7.4524		7.1671
KYM		7.3381		7.1346
LM		7.339		7.1554
RFE		7.4015		7.1563
TM		7.3406		7.159
VDPO		7.3179		7.1438

4. CONCLUSION

The performance analysis of some of the available chaotic maps with at least two dimensions in data security application proves the practicality of using chaotic maps in cryptosystems, specifically in image encryption.

The almost flat histogram of all the chaos-based encryption system signifies their good diffusion characteristic. The scattered pattern in the correlation coefficient plot and high entropy value of all the studied scheme proves its good confusion characteristic. And the key sensitivity analysis, which shows an unrecognizable image, even though the key was just changed by a mere .001 in value, showcases the strong avalanche property of the studied systems.

In addition, this study also proves that the incorporation of a simple fuzzy logic algorithm to the encryption process, in fact, improves the schemes level of security as indicated in Table 4.

5. REFERENCES

[1] Habutsu, T., Nishio, Y., Sasase, I., & Mori, S. (1998). *A Secret Key Cryptosystem by Iterating a Chaotic Map.* Yokohama: Dept. EE, Keio University, Springer- Verlag.

[2] Parliamentary Office of Science and Technology. (October 2006). *Data Encryption.* London: Parliamentary Office of Science and Technology.

[3] Blackledge, J. (March 2010). *Cryptography using Chaos.* Warsaw: Warsaw University of Technology.

[4] Roskin, K., & Casper, J. (1999). *From Chaos to Cryptography.* Santa Cruz: University of California.

[5] Ross, T. J. (2010). *Fuzzy Logic With Engineering Applications.* West Sussex: John Wiley & Sons, Ltd.

[6] ELabbasy, E. M., Agiza, H. N., EL-Metwally, H., & A., E. A. (2007). Bifurcation Analysis, Chaos and Control in the Burgers Mapping. *International Journal of Nonlinear Science*, 171.

[7] Forssen, P.-E. (1999). *Image Analysis using Soft Histograms.* Lingkoping: Dept. EE, Lingkopoing University.

[8] Callaghan, K. P. (2000). *The Correlation Coefficient.* Boston: University of Massachusetts.

[9] Aboites, V., & Mario, W. (2009). TINKERBELL CHAOS IN A RING PHASE-CONJUGATED RESONATOR. *International Journal of Pure and Applied Mathematics*, 430.

[10] J. A. Martínez-Ñonthe, A. D.-M.-I.-L.-R.-C.-M. (2011). *Cryptosystem with One Dimensional Chaotic Maps.* Torremolinos-Málaga, Spain: Springer Berlin Heidelberg.

[11] Kantz, H., & Schreiber, T. (1998). *NONLINEAR PROJECTIVE FILTERING I: BACKGROUND IN CHAOS THEORY.* Wuppertal.

[12] Luo, X., Small, M., Danca, M. F., & Chen, G. (2007). ON A DYNAMICAL SYSTEM WITH MULTIPLE CHAOTIC ATTRACTORS. *International Journal of Bifurcation and Chaos,*, 3237.

[13] Nguyen, C. (2009). *Van der Pol Oscillators Synchronization: Methods and Applications.* Yale.

[14] Otsubo, K., Washida, M., Itoh, T., Katsuura, K., & Hayashi, M. (2000). *Computer Simulation on the Gumowski-Mira Transformation.* Tokyo.

[15] Abuhaiba, I. S., AlSallut, A. Y., Hejazi, H. H., & AbuGhali, H. A. (2012). *Cryptography Using Multiple Two-Dimensional Chaotic Maps.* Gaza, Palestine: MECS.

[16] Parsopoulos, K. E., & Vrahatis, M. N. (2003). *Computing Periodic Orbits of Nondifferentiable/Discontinuous Mappings Through Particle Swarm Optimization.*

[17] Rojas, J. (1996). *Fuzzy Logic.* Berlin: Springer-Verlag.

[18] Frigg, R., & Werndl, C. (June 2010). *Entropy - A Guide for the Perplexed.*

[19] Denning, D. E., & Denning, P. J. (1979). *Data Security.* Indiana: CS Department, Purdue University.

[20] Singh, K., & Kaur, K. (2011). Image Encryption using Chaotic Maps and DNA Addition Operation and Noise Effects on it. *International Journal of Computer Applications*, 17 - 18.

[21] Siska, A. (2009). *Chaos: Another Tool for Synthesis.* Budapest.

[22] Soler, V. B., Castelo, J. M., Oteo, J. A., & Ros, J. (2011). *Bifurcations in the Lozi map.* Valencia, Spain.

[23] Wronka, A. E. (2011). *Separatrix Splitting for the Extended Standard Family of Maps.* Edinburgh.

[24] Zhang, L., & Liao, X. W. (September 2004). *An image encryption approach based on chaotic maps.* Chongqing: Chongqing University.

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