Improving Chaotic Image Encryption Using Maps with Small Lyapunov Exponents

Thiago A. Santos
Electrical Engineering Department
Federal University of São João del-Rei
São João del-Rei, Brazil
contato@tsantos.com.br

Eduardo P. Magalhães
Electrical Engineering Department
Federal University of São João del-Rei
São João del-Rei, Brazil
eduardopintomagalhaes@gmail.com

Nayara P. Basílio
Electrical Engineering Department
Federal University of São João del-Rei
São João del-Rei, Brazil
nayarabasilio@hotmail.com

Erivelton G. Nepomuceno
Electrical Engineering Department
Federal University of São João del-Rei
São João del-Rei, Brazil
nepomuceno@ufsj.edu.br

Timur I. Karimov
Computer Aided Design Department
Petersburg Electrotechnical University
Saint-Petersburg, Russia
tikarimov@etu.ru

Denis N. Butusov
Youth Research Institute
Petersburg Electrotechnical University
Saint-Petersburg, Russia
dnbutusov@etu.ru

***Abstract*—Chaos-based encryption is one of the promising cryptography techniques that can be used. Although chaos-based encryption provides excellent security, the finite precision of number representation in computers affects decryption accuracy negatively. In this paper, a way to mitigate some problems regarding finite precision is analyzed. We show that the use of maps with small Lyapunov exponents can improve the performance of chaotic encryption scheme, making it suitable for image encryption.**

Keywords—encryption, chaotic systems, finite precision, lower bound error, largest Lyapunov exponent, Shannon entropy

I. INTRODUCTION

Chaotic oscillators allow generating pseudo-random sequences indistinguishable from truly random sequences, that provide high level of their encryption security [1].Such property of dynamical chaos as determinism makes it possible to conceal information using chaotic time series in a manner that it can be recovered later. In its simplest form, chaos-based cryptography uses a pseudo-random number sequence as a key that modifies the data by XOR binary operation. Nevertheless, encryption using this technique and its more sophisticated modifications often leads to unsatisfactory quality of decrypted data caused by numerical errors during decryption procedure [2-4].

The largest Lyapunov exponent is a measure of the chaotic system divergence rate from the close initial conditions. It is known that systems with large Lyapunov exponents are difficult to simulate, in contrast to systems with small Lyapunov exponents, which numerical solutions are close to analytical over large time intervals. This leads to the idea of reducing the decryption error by using chaotic systems whose numerical solution error is lower, i.e. systems with smaller LLEs. Our experiments with simple XOR-based chaotic encryption scheme confirm the hypothesis. Although many valuable additions to the simple technique under study have been made, our results seem to be fundamental relative to any of the more advanced methods.

The paper is organized as follows. In Section II, we introduce some basic definitions and concepts. Section III describes the methodology of the investigation in details. Section IV presents summary of the findings and Section V concludes the paper.

The reported study was partially supported byCNPq, FAPEMIG, CAPES. Denis N. Butusov was supported by the grant of the Russian Science Foundation (RSF), project № 19-71-00087.

II. PRELIMINARY CONCEPTS

A. Orbits, pseudo-orbits and lower bound error

Definition 1.An orbit is a sequence of map values:

$$\{x_n\} = [x_1, x_2, x_3, ...x_n].$$

Definition 2. A pseudo-orbit is an approximation of an orbit given by:

$$\hat{X}_{i,n} = \hat{x}_{i,0}, \hat{x}_{i,1}, \hat{x}_{i,2}, ..., \hat{x}_{i,n},$$

such that

$$\left| x_n - \hat{x}_{i,n} \right| \le \delta_{i,n},$$

where $\delta_{i,n} \in \Re, \delta_{i,n} \ge 0$ .Pseudo-orbits define the interval in which the true orbit is located.

B. Lower bound error

The lower bound error (LBE) is a measure of the computational error accumulating at each iteration of the numerical simulation. It is given by theorem.

Theorem 1. Let two pseudo-orbits $\{\hat{x}_{a,n}\}$ and $\{\hat{x}_{b,n}\}$ be derived from two interval extensions. Also, let $\delta_{a,n} = \frac{1}{2}\left|\hat{x}_{a,n} - \hat{x}_{b,n}\right|$ be the lower bound error of a map $f(x)$ .Then $\delta_{b,n} \ge \delta_{a,n}$.

where *a* and *b* are indices indicating different extensions. The proof of Theorem 1 can be found in [6]. The definition of LBE states that at least one of two pseudo-orbits must have an error greater than or equal to the lowest error.

C. Shannon Entropy

Shannon entropy H is given by the following equation:

978-1-7281-2572-5/20/$31.00 ©2020 IEEE

$$H(x) = -\sum_{i=0}^{N-1} P_i \log_2(P_i) \quad (4)$$

where P_i is the probability of number i to appear in any position of the message. Normalized Shannon entropy function outputs values from 0 to 1, where the higher number corresponds to the higher entropy value:

$$H_{norm} = -\frac{H \log_2(2)}{\log_2(N)} \quad (5)$$

D. The largest Lyapunov exponent calculation

By using simple method described in [5], it is possible to calculate the LLE by simulating two interval extensions of the same pseudo-orbit and find the lower bound error between them.

In this work, the LLE is calculated by averaging the slope of the lower bound error plot, as proposed in [5]. To verify the result, LLE was also calculated using the Kantz method in software called "*Lyap_k*" [7]. The algorithm developed by Kantz is based on equation (6):

$$S(k) = \frac{1}{N}\sum_{i=1}^{N} \ln\left(\frac{1}{|\eta(x_i)|}\sum_{x'_i \in \eta(x_i)} |x_{i+k} - x'_{i+k}|\right), \quad (6)$$

where N is the total number of points and the diameter of the neighborhood $\eta(x_i)$ is preliminarily defined. LLE is given by the approximation the slope line in the logarithmic scale plot, as shown in Fig. 1. The exponent is determined by the median of the inclination of the five straight lines. The standard deviation to prove it is validity was also calculated.

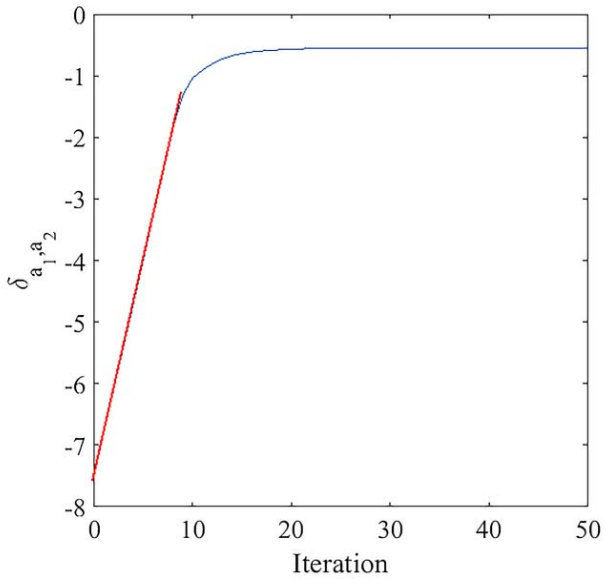

Fig. 1. Example of a LLE calculation using Kantz's method.

E. Calculation of Pearson correlation coefficient

To determine the security of image encryption and accuracy of its decryption, the Pearson correlation coefficient was calculated between obtained data series. Equation (7) introduces the appropriate formula.

$$\rho(X,Y) = \frac{E[(X-\mu x)(Y-\mu y)]}{\sigma x \sigma y} \quad (7)$$

The correlation coefficient (7) ranges from −1 to 1. A value of 1 corresponds to the case when a linear equation fits the relationship between X and Y perfectly, with all data points lying on a line for which Y increases as X increases. A value of −1 corresponds to the case when all data points lie on a line for which Y decreases as X increases. A value of 0 when there is no linear correlation between the variables.

III. Methodology

In the current research, encrypting and decrypting of the test image were performed at different LLE values to evaluate which value gives a more accurate decryption result. IEEE754 format was used to represent floating point numbers. In the experiments, a standard 8-bit black-and-white Lena image was used, see Fig. 2 [8]. It was encoded with a matrix of 256 × 256 pixels, each position in the matrix stored the value of a grayscale pixel from 0 to 255 [5]. A cubic mapping [9] of the interval $[-1, 1]$ was used as a chaotic system:

$$f(x) = ax^3 + (1-a)x \quad (8)$$

In total, 5 different parameter values of the mapping (8)were tested. Encrypted images were generated by multiplying each iteration of the chaotic map by a coefficient and using it as input for the next iteration. The results were then analyzed using LLE estimation and Shannon entropy analysis. Since the symmetric encryption scheme was implemented, the key had the same size as the image (9).

$$[\text{Results}]=256*|[\text{Results}]| \quad (9)$$

Coefficients from 0.9 to 1 with steps of 0.02 were chosen to reduce the LLE. By multiplying each iteration and using it as input to the next, one can get lower values of the LLE (10).

$$x_{n+1} = pf(x_n), \quad p \in \overline{0.9..1} \quad (10)$$

Although, this is an effective method, care should be taken to ensure that the output remains chaotic.

Fig. 2. Since 1973, Lena is the standard image for testing image processing and encryption algorithms. We use a grayscale image with size of 256 × 256 pixels.

Two simulations were made for each coefficient. The first one had its initial condition set to 0.1, and the second one to 0.2. Each simulation filled half of the key, to allow shorter simulation sizes and avoid much computational error propagation. Also, for each simulation, a different interval obtained from arithmetic properties was calculated in order to evaluate the lower bound error.

The lower bound error was calculated in order to estimate LLEs. After applying the LBE formula, the resulting vectors were analyzed for the first peak, and aslope line was approximated with the Least Squares method. The slope value of this line defines the LLE value, see Fig. 3. The LLE was also calculated by Kantz's method in order to compare the results. The standard deviation was also found to prove it is validity.

Shannon entropy was used analyzed as a mean to quantify the confusion levels of each encrypted image.

IV. Results

A. Lower bound error

The lower bound error was calculated to ensure that each simulation was chaotic. If the initial slope of the lower bound error plot is positive, the LLE is positive, which means the system output sequence is chaotic.

B. Largest Lyapunov exponent

The LLE was calculated by means of the Nepomuceno and Kantz methods. The results can be seen in the Fig. 3 and Table I. One can note that the values found have small standard deviations, and as the coefficient increase the Lyapunov exponent increase.

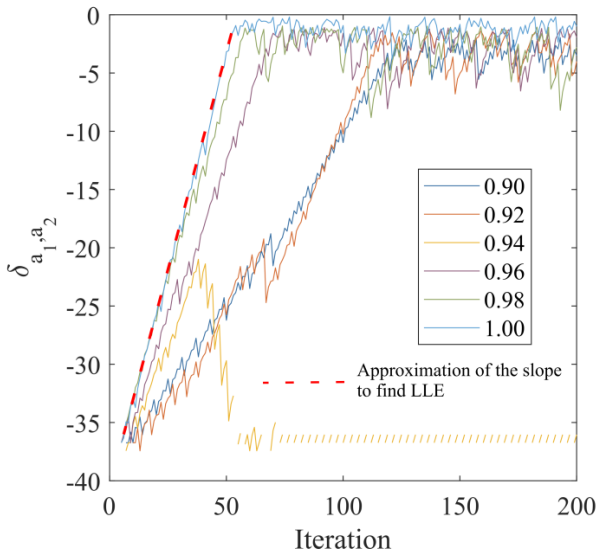

Fig. 3. Comparison of various lower bound error plots for each of the coefficients. The LLE follows the slope of the lower bound error line. For coefficients closer to one, the LLE is higher.When using the coefficient as 0.94, the map does not present chaos and corresponding time sequence cannot be used for high-security encryption.

TABLE I. Largest Lyapunov Exponent Calculated for the Time Series

Coefficient	λ1 ± 3σ (Kantz), bits/iteration	λ2 (Nepomuceno), bits/iteration
0.90	0.4925±0.0795	0.2904
0.92	0.3961±0.0366	0.3172
0.94	not chaotic	not chaotic
0.96	0.6571±0.0303	0.5389
0.98	0.7521±0.0648	0.6510
1.00	0.9729±0.0783	0.7211

C. Decryption results

The decryption results confirmed that the process can be enhanced by using smaller Lyapunov exponents. For encrypted images see Fig. 4.

D. Correlation coefficient

The correlation coefficient formula was applied to evaluate how the encrypted and decrypted images are related, and how the encrypted and original images are related. The results are summarized in Table II.

It can be seen from Table II, that with a smaller coefficient the LLE decreases. Also, for smaller values of the coefficient, the original image correlates more with the decrypted image. For the 0.94 coefficient, data should't be considered, since the time sequence was not chaotic.

TABLE II. STATISTICAL RELATIONSHIP BY CALCULATING THE CORRELATION COEFFICIENT BETWEEN THE ORIGINAL AND ENCRYPTED IMAGE, AND BETWEEN THE ORIGINAL AND THE DECRYPTED IMAGE

Coefficient	LLE	Original ↔ Encrypted	Original ↔ Decrypted
0.90	0.2904	-0.229760	0.141822
0.92	0.3172	-0.278381	0.140696
0.94	not chaotic	0.253779	-0.229420
0.96	0.5389	-0.026341	0.002367
0.98	0.651	0.018259	0.006331
1.00	0.7211	0.075895	0.002459

V. CONSLUSION

In this work, we analyze how the largest Lyapunov exponent influences the chaos-based cryptography. A very simple Lyapunov exponent control scheme suitable for any chaotic interval mapping was proposed. From the experimental results if follows that smaller positive Lyapunov exponents enhance the decryption process, showing better preservation of accuracy. Selection of proper Lyapunov exponent value can increase Pearson correlation coefficient between the original and decrypted images up to 0.3. Obtained improvement is a necessary step towards the wide implementation of chaos-based encryption.

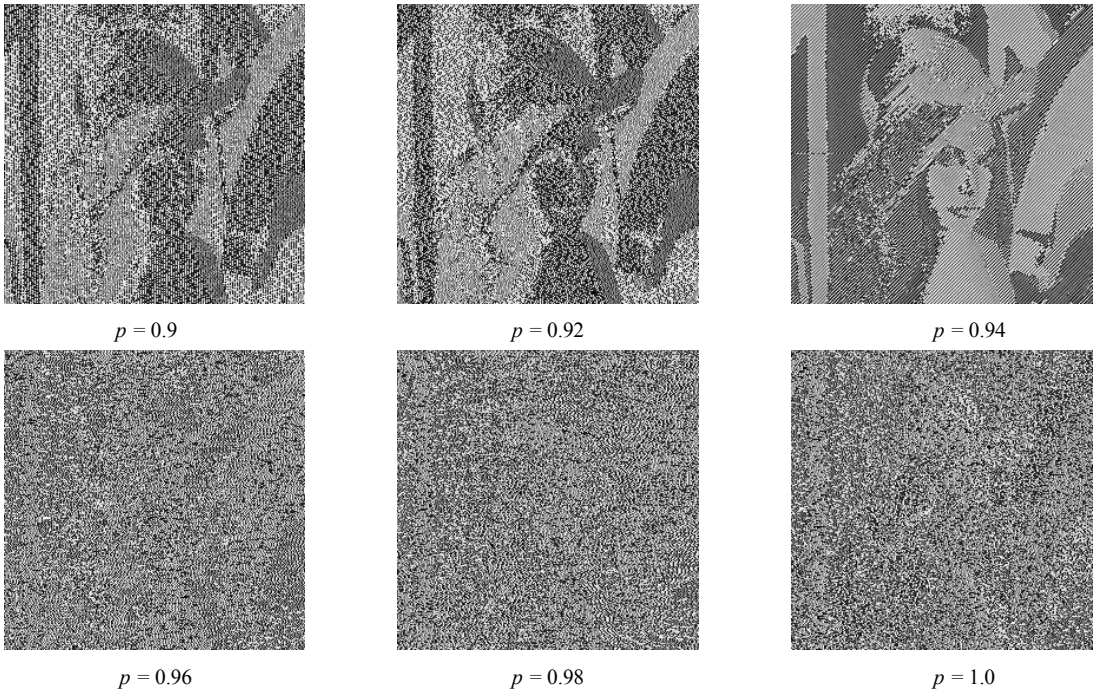

Fig. 4. Images encrypted by the pseudo-orbit of map (8) in ascending order of the coefficient (10).

As a limitation of the study we can cite that the only one chaotic mapping was used in the current study. In future work, we will consider other chaotic mappings for random sequences generation.

REFERENCES

[1] A.V. Tutueva, D.N. Butusov, D.O. Pesterev, D.A. Belkin, N.G. Ryzhov, "Novel normalization technique for chaotic pseudo-random number generators based on semi-implicit ODE solvers," 2017 International Conference on Quality Management, Transport and Information Security, Information Technologies (IT&QM&IS), Saint Petersburg, Russia, pp. 284-287, Sept. 2017.

[2] T.A. Santos, E.P. Magalhaes, D.R. Fiorio, E.G. Nepomuceno, "On the reliability of computational chaos-based cryptography for information exchange," Oct. 2019.

[3] L.G. Nardo, E.G. Nepomuceno, J. Arias-Garcia, D. N. Butusov, "Image encryption using finite-precision error," Chaos, Solitons and Fractals, vol. 123, pp. 69–78, Jun. 2019.

[4] E.G. Nepomuceno, L. G. Nardo, J. Arias-Garcia, D. N. Butusov, A. Tutueva, "Image encryption based on the pseudo-orbits from 1D chaotic map," Chaos, vol. 29, no. 6, Jun. 2019.

[5] A.M. Mendes, E.G. Nepomuceno, "A Very Simple Method to Calculate the (Positive) Largest Lyapunov Exponent Using Interval Extensions," Int. J. Bifurc. Chaos, vol. 26, no. 13, p. 1650226, Dec. 2016.

[6] E.G. Nepomuceno, S.A.M. Martins, "A lower bound error for free-run simulation of the polynomial NARMAX," Syst. Sci. Control Eng., vol. 4, no. 1, pp. 50–58, Jan. 2016.

[7] H. Kantz, "A robust method to estimate the maximal Lyapunov exponent of a time series," Phys. Lett. A, vol. 185, no. 1, pp. 77–87, Jan. 1994.

[8] I.V. Bogach, D.D. Lupiak, Yu.Yu. Ivanov, O.V. Stukach, "Analysis and Experimental Research of Modifications of the Image Segmentation Method Using Graph Theory". 2019 International Siberian Conference on Control and Communications (SIBCON). 18-20 April 2019, Russia. DOI: 10.1109/SIBCON.2019.8729659.

[9] T.D. Rogers, D.C. Whitley, "Chaos in the cubic mapping," Mathematical Modelling,Vol. 4, Issue 1, pp. 9-25, 1983.