CHAOS
Theory and Applications
in Applied Sciences and Engineering

e-ISSN: 2687-4539
RESEARCH ARTICLE
Vol.4 / No.4 / 2022 / pp.274-284
Special Issue (EDIESCA 2022)
https://doi.org/10.51537/chaos.1214569

A Chaotification Model Based on Modulo Operator and Secant Functions for Enhancing Chaos

Nikolaos Charalampidis[*], **Christos Volos**[*], **Lazaros Moysis**[*,β] **and Ioannis Stouboulos**[*]

[*]Laboratory of Nonlinear Systems - Circuits & Complexity, Physics Department, Aristotle University of Thessaloniki, Thessaloniki, Greece, [β]Department of Mechanical Engineering, University of Western Macedonia, Kozani, Greece.

ABSTRACT Many drawbacks in chaos-based applications emerge from the chaotic maps' poor dynamic properties. To address this problem, in this paper a chaotification model based on modulo operator and secant functions to augment the dynamic properties of existing chaotic maps is proposed. It is demonstrated that by selecting appropriate parameters, the resulting map can achieve a higher Lyapunov exponent than its seed map. This chaotification method is applied to several well-known maps from the literature, and it produces increased chaotic behavior in all cases, as evidenced by their bifurcation and Lyapunov exponent diagrams. Furthermore, to illustrate that the proposed chaotification model can be considered in chaos-based encryption and related applications, a voice signal encryption process is considered, and different tests are being used with respect to attacks, like brute force, entropy, correlation, and histogram analysis.

KEYWORDS
Chaotic map
Chaotification
Secant functions
Modulo operator
Lyapunov exponent
Sound encryption
Fuzzy entropy

INTRODUCTION

Chaos theory, as a mathematical discipline aims to study the dynamic behavior of systems that are highly sensitive to the initial conditions and parameter values (Grassi 2021). Chaos can be found basically in almost all fields from natural and social sciences, to engineering, and medicine, even economics (Nagashima *et al.* 2019). As a result chaos theory has evolved to a large attraction for researchers, and the past decades is continuously being studied, due to a number of appealing characteristics such as randomness, and unpredictability, nonlinearity, and initial condition sensitivity, which over the years led to many interesting and varying applications. Examples of chaos applicability can be found in robotics (Petavratzis *et al.* 2022), weather forecast (Mammedov *et al.* 2022), pandemic crisis management (Borah *et al.* 2022), information security (Fadil *et al.* 2022), circuits (Xiu *et al.* 2022), and signal processing (Abd *et al.* 2022).

Generally in chaos-based applications, and in particular cryptography, better chaotic properties are imperative, since they imply enhanced performance or security. However, many classic chaotic maps like the logistic map and the sine map exhibit weaknesses. For instance, simple phase portraits which makes it easy to identify their equilibrium points. This allows potential attackers to predict the chaotic sequence and the parameter values just by analyzing the equilibrium points (Shahi *et al.* 2022; Wang *et al.* 2022). Another example is low chaos complexity, which in turn leads to degradation of the chaotic behavior (Liu *et al.* 2021). Furthermore, small regions of chaos also constitutes a weakness, since within an interval of the control parameter values, only a subset is admitted for use, leading to limited applicability of the chaotic map (Zeraoulia 2012). Consequently, achieving strong chaos with enhanced performance has the potential to vastly improve chaos theory research into the development of related applications.

In this direction, optimization methods to increase Lyapunov exponents of chaotic systems are developed, for example via differential evolution and particle swarm optimization algorithms (de la Fraga *et al.* 2012; Adeyemi *et al.* 2022). The reason for that is because the Lyapunov exponent measures the sensitivity of the initial conditions for a chaotic map to small changes (Bovy 2004). Additionally, since positive Lyapunov exponent values indicate chaos, the higher they are the more complex a chaotic system is regarded.

Furthermore, as of recent, there is a movement to develop families of chaotic systems, often called chaotification models (Moysis *et al.* 2022a), that holistically improve the chaotic behavior for any given existing chaotic map. To do so, the goal is to prove that a

Manuscript received: 5 December 2022,
Revised: 22 December 2022,
Accepted: 27 December 2022.

[1]nicharala@physics.auth.gr (**Corresponding author**)
[2]volos@physics.auth.gr
[3]lmousis@physics.auth.gr
[4]stouboulos@physics.auth.gr

chaotification model can achieve higher Lyapunov exponent values than the existing chaotic maps, and verify that with numerical experiments. Such examples are to combine any map with a cosine function (Natiq *et al.* 2019), a sine function (Hua *et al.* 2018), a sine and cosecant functions (Li *et al.* 2021), a cascade sine operation (Wu 2021), an internal perturbation model (Dong *et al.* 2021), a remainder operation addition (Moysis *et al.* 2022b), or the modulo operator, which has been shown to be effective in improving chaotic behavior (Ablay 2022; Zhang *et al.* 2022).

Influenced by this, a chaotification model based on the modulo operation and secant function to strengthen the complexity of existing chaotic maps is constructed. Its structure is comprised of the secant function, which influences directly the output of existing chaotic maps, acting as a chaotification agent, and the modulo operator, which limits the set of possible output values. To assess the model's performance, a theoretical analysis based on the Lyapunov exponent is conducted. Additionally, four one-dimensional chaotic maps acting as seed maps are applied to the model, leading to four new chaotic maps. The chaos complexity of these maps is then evaluated through common tools for studying the dynamical behavior of chaotic systems, namely phase, bifurcation, Lyapunov exponent diagrams, and the fuzzy entropy.

Moreover, to illustrate an application of the proposed chaotification model, a voice signal encryption technique is designed based on one of the new chaotic maps. This map is used to shuffle, and modulate the signal to obtain the ciphered signal. This voice signal encryption technique's security is validated and tested using a variety of tests and measures such as histogram, and key space and sensitivity analysis, approximate entropy, spectral distortion, log-likelihood, and signal to noise ratio.

The outline of the paper is as follows: Section 2 presents the proposed chaotification model, and the theoretical analysis of its performance. Section 3 introduces four new chaotic maps. In Section 4 the dynamics of the new maps is discussed. Section 5 considers the application of voice encryption. In Section 6 the encryption performance is discussed. Section 7 conclusions are presented, along with a suggestion for future research based on the shortcomings of the suggested model.

CHAOTIFICATION MODEL BASED ON MODULO OPERATOR AND SECANT FUNCTIONS

In this section is introduced the proposed chaotification model and are presented various examples of modified chaotic maps to illustrate the model's effectiveness.

Concept of the chaotification model

The proposed chaotification model uses a double nonlinear transformation based on the modulo operator and secant function to improve the chaotic properties and complexity of existing chaotic maps as shown in Fig. 1.

Consider the modulo operator $\mod(\cdot, N)$, and the secant function $sc(\cdot) = \frac{1}{\cos(\cdot)}$, then the chaotic system is of the following form:

$$x_{i+1} = mod(a \cdot sc(b \cdot F(x_i)), N) \tag{1}$$

where x_i is the input, $a, b \in \mathbb{R}^+$ are the system's parameters, $F(x_i)$ the existing chaotic maps, and $N \in \mathbb{N}^*$ the control parameter that limits the map's values in the interval $[0, N]$.

The following aspect primarily reflects the augmentation of the chaotic complexity of the resulting new maps. The chaotification model expands the chaotic range of one dimensional chaotic

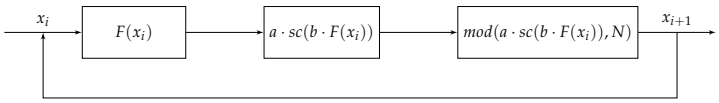

Figure 1 Structure of the chaotification model based on modulo operator and secant functions.

maps. Meaning that the modified maps have larger control parameter range than before. This will be confirmed theoretically and experimentally.

Lyapunov exponent analysis

One of the most well-known tools for studying the quantitative behavior of chaotic systems is the Lyapunov exponent. The Lyapunov exponent for a dynamical system of the form $x_{i+1} = f(x_i)$ is defined as follows:

$$\lambda = \lim_{n\to\infty} \frac{1}{n} \sum_{i=0}^{n-1} \ln \mid \dot{f}(x_i) \mid \tag{2}$$

When $\lambda > 0$ implies existence of chaos. Furthermore, a greater Lyapunov exponent is an indication of a more complex chaotic behavior.

By the definition of Lyapunov exponent a chaos complexity analysis of the proposed chaotification method can be derived. The derivative in Eq. (2) is known that is the slope of the tangent line at any given point $(x_i, f(x_i))$ of the chaotic system's curve. In addition, the modulo operator has an inherent property that allows it to translate a curve's part that is outside the phase space inside of it without alterations.

Therefore, without loss of generality, the modulo operator can be disregarded, and the chaotification model in (1) be regarded as

$$x_{i+1} = \mathcal{M}(x_i) = a \cdot sc(b \cdot F(x_i)). \tag{3}$$

Hence, the following theorem is proven.

Theorem 1. *The proposed map (1) achieves a higher Lyapunov exponent (LE) compared to its source map $F(x_i)$, for appropriate choice of parameters a, b.*

Proof. This proof is inspired by (Zhang *et al.* 2022; Li *et al.* 2021). Consider two initial conditions y_0 and x_0, where x_0 differs from y_0 by a small number $\epsilon > 0$. Then, after iterating once are obtained y_1 and x_1. Their difference is computed as follows,

$$\begin{aligned}
&|y_1 - x_1| = |\mathcal{M}(y_0) - \mathcal{M}(x_0)| \\
&= |a \cdot sc(b \cdot F(y_0)) - a \cdot sc(b \cdot F(x_0))| \\
&= \left| \left(\frac{a \cdot sc(b \cdot F(y_0)) - a \cdot sc(b \cdot F(x_0))}{F(y_0) - F(x_0)} \right) \left(\frac{F(y_0) - F(x_0)}{y_0 - x_0} \right) (y_0 - x_0) \right| \\
&= \left| \left(\frac{a \cdot sc(b \cdot F(y_0)) - a \cdot sc(b \cdot F(x_0))}{F(y_0) - F(x_0)} \right) \right| \left| \left(\frac{F(y_0) - F(x_0)}{y_0 - x_0} \right) \right| |y_0 - x_0|.
\end{aligned} \tag{4}$$

Because from hypothesis $y_0 \to x_0$, consequently $F(y_0) \to F(x_0)$, then

$$\lim_{y_0 \to x_0} \left| \left(\frac{F(y_0) - F(x_0)}{y_0 - x_0} \right) \right| \approx \frac{dF}{dx}|_{x_0}$$

$$\lim_{F(y_0) \to F(x_0)} \left| \left(\frac{a \cdot sc(b \cdot F(y_0)) - a \cdot sc(b \cdot F(x_0))}{F(y_0) - F(x_0)} \right) \right| \approx \frac{d\mathcal{M}}{dx}|_{F(x_0)}$$

Therefore,

$$|y_1 - x_1| \approx \left|\frac{d\mathcal{M}}{dx}|_{F(x_0)}\right| \left|\frac{dF}{dx}|_{x_0}\right| |y_0 - x_0|. \tag{5}$$

In similar way, after iterating for a second time y_2 and x_2 are obtained. Their difference is calculated as

$$\begin{aligned}
&|y_2 - x_2| = |\mathcal{M}(y_1) - \mathcal{M}(x_1)| \\
&= |a \cdot sc(b \cdot F(y_1)) - a \cdot sc(b \cdot F(x_1))| \\
&= \left|\left(\frac{a \cdot sc(b \cdot F(y_1)) - a \cdot sc(b \cdot F(x_1))}{F(y_1) - F(x_1)}\right)\left(\frac{F(y_1) - F(x_1)}{y_1 - x_1}\right)(y_1 - x_1)\right| \\
&= \left|\left(\frac{a \cdot sc(b \cdot F(y_1)) - a \cdot sc(b \cdot F(x_1))}{F(y_1) - F(x_1)}\right)\right| \left|\left(\frac{F(y_1) - F(x_1)}{y_1 - x_1}\right)\right| |y_1 - x_1| \\
&\approx \left|\frac{d\mathcal{M}}{dx}|_{F(x_1)}\right| \left|\frac{dF}{dx}|_{x_1}\right| \left|\frac{d\mathcal{M}}{dx}|_{F(x_0)}\right| \left|\frac{dF}{dx}|_{x_0}\right| |y_0 - x_0|.
\end{aligned} \tag{6}$$

After iterating for the n^{th} time and y_n and x_n are obtained, their difference can be computed as

$$\begin{aligned}
|y_n - x_n| &= |\mathcal{M}(x_{n-1}) - \mathcal{M}(x_{n-1})| \\
&\approx \prod_{i=0}^{n-1} \left|\frac{d\mathcal{M}}{dx}|_{F(x_i)} \frac{dF}{dx}|_{x_i}\right| |y_0 - x_0|.
\end{aligned} \tag{7}$$

The average divergence after n iterations will be denoted $\Delta_{\mathcal{M}}(x)$, and is calculated as follows:

$$\begin{aligned}
\Delta_{\mathcal{M}(x)} &= \left|\frac{y_n - x_n}{y_0 - x_0}\right|^{\frac{1}{n}} \\
&= \left(\prod_{i=0}^{n-1} \left|\frac{d\mathcal{M}}{dx}|_{F(x_i)} \frac{dF}{dx}|_{x_i}\right|\right)^{\frac{1}{n}}
\end{aligned} \tag{8}$$

Hence, from equation (2) the Lyapunov exponent of $\lambda_{\mathcal{M}(x)}$ can be obtained.

$$\begin{aligned}
\lambda_{\mathcal{M}(x)} &= \lim_{n\to\infty} \ln(\Delta_{\mathcal{M}(x)}) \\
&= \lim_{n\to\infty} \frac{1}{n} \ln\left(\prod_{i=0}^{n-1} \left|\frac{d\mathcal{M}}{dx}|_{F(x_i)} \frac{dF}{dx}|_{x_i}\right|\right) \\
&= \lim_{n\to\infty} \frac{1}{n} \sum_{i=0}^{n-1} \ln\left|\frac{d\mathcal{M}}{dx}|_{F(x_i)} \frac{dF}{dx}|_{x_i}\right| \\
&= \lim_{n\to\infty} \frac{1}{n} \sum_{i=0}^{n-1} \ln\left|\frac{ab\dot{F}(x_i)\sin(bF(x_i))}{\cos^2(bF(x_i))}\right| \\
&= \lim_{n\to\infty} \frac{1}{n} \sum_{i=0}^{n-1} \left(\ln|ab\dot{F}(x_i)\sin(bF(x_i))| - \ln\left|\cos^2(bF(x_i))\right|\right) \\
&= \lim_{n\to\infty} \frac{1}{n} \sum_{i=0}^{n-1} \left(\ln|ab\dot{F}(x_i)\sin(bF(x_i))|\right) \\
&\quad - \lim_{n\to\infty} \frac{1}{n} \sum_{i=0}^{n-1} \left(\ln\left|\cos^2(bF(x_i))\right|\right) \\
&= \lambda + \ln|a| + \lim_{n\to\infty} \frac{1}{n} \sum_{i=0}^{n-1} \left(\ln|b\sin(bF(x_i))|\right) \\
&\quad - \lim_{n\to\infty} \frac{1}{n} \sum_{i=0}^{n-1} \left(\ln\left|\cos^2(bF(x_i))\right|\right) \\
&= \lambda + \ln|\,a\,| + \lambda_{\mathcal{C}(x)} + \gamma
\end{aligned} \tag{9}$$

where

$$\lambda = \lim_{n\to\infty} \frac{1}{n} \sum_{i=0}^{n-1} \ln|\dot{F}(x_i)|,$$

$$\gamma = -\lim_{n\to\infty} \frac{1}{n} \sum_{i=0}^{n-1} \left(\ln\left|\cos^2(bF(x_i))\right|\right),$$

and

$$\lambda_{\mathcal{C}(x)} = \lim_{n\to\infty} \frac{1}{n} \sum_{i=0}^{n-1} \left(\ln|b\sin(bF(x_i))|\right)$$

Notice that since $0 \le \cos^2(b(F(x_i))) \le 1$ then $\gamma \ge 0$, and $\ln|a| > 0$ iff $a > 1$. Furthermore, it can be noticed that $\ln|b\sin(bF(x_i))| > 0$ iff $|b\sin(bF(x_i))| > 1$ as such $|b| > \frac{1}{|\sin(bF(x_i))|}$, and because $b \in \mathbb{R}^+$, $b > \frac{1}{|\sin(bF(x_i))|}$. Thus, $\lambda_{\mathcal{C}(x)} > 0$ if and only if, $b > \frac{1}{|\sin(bF(x_i))|}$. However, because b is depended on $F(x_i)$ it is very difficult to identify a particular set of values for b from this condition.

Similarly to (Li *et al.* 2021) in order to identify values for the parameter b such that $\lambda_{\mathcal{C}(x)} > 0$, design the chaotic map

$$x_{i+1} = -\cos(bx_i). \tag{10}$$

with corresponding Lyapunov exponent

$$\lim_{n\to\infty} \frac{1}{n} \sum_{i=0}^{n-1} \left(\ln|b\sin(bx_i)|\right)$$

According to the bifurcation and Lyapunov exponent diagram of Eq. (10) depicted in Fig. 2, the map exhibits chaotic behavior with respect to parameter b for a variety of values. For example, $b = 1$ or 20. Thus, it can be concluded that for the same value of parameter b, $\lambda_{\mathcal{C}(x)} > 0$.

Hence, the chaotic properties based on the above analysis can be summarized as follows:

1. When $\lambda > 0$ and $\lambda_{\mathcal{M}(x)} > \lambda > 0$. In this case, the generated new map shows chaos and has larger Lyapunov exponent than the seed map.

2. If $\lambda < 0$, and $\lambda > -(\lambda_{\mathcal{C}(x)} + \gamma + \ln|a|)$. In this case also the generated new map shows chaos.

3. When $\lambda < 0$, and $\lambda \le -(\lambda_{\mathcal{C}(x)} + \gamma + \ln|a|)$. Then the generated new map does not have chaotic behavior.

Hence, it has been proved that the proposed chaotification model can improve the complexity of the seed map and the modified map can obtain larger Lyapunov exponents.

EXAMPLES OF NEW CHAOTIC MAPS

To showcase our previous result, the logistic map, the sine map, the sine sine map, and the cosine logistic map are used as seeds, yielding four new chaotic maps of the form (1). It should be noted that all initial conditions are set $x_0 = 0.1$. Furthermore, the parameter b when directly multiplied with a seed map's control parameter is set $b = 1$, if not then b can take any positive real number under the condition that the value of b is within a chaotic region of the map $x_{i+1} = -\cos(bx_i)$.

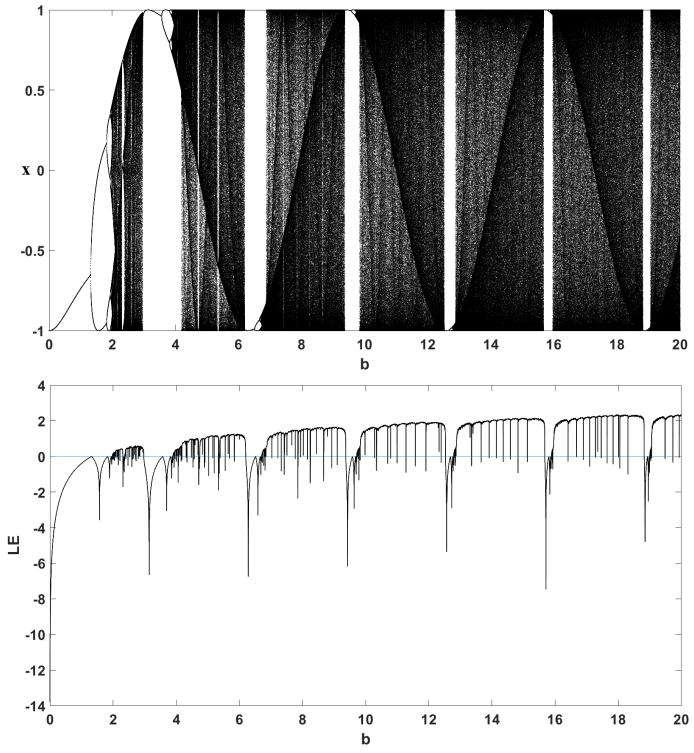

Figure 2 The bifurcation and Lyapunov exponent diagram of Eq. (10) with respect to b.

Modified logistic map

Consider the Logistic map $F(x_i) = rx_i(1 - x_i)$ as a seed map to Eq. (1), then the following map is obtained:

$$x_{i+1} = mod(a \cdot sc(brx_i(1 - x_i)), N) \tag{11}$$

Modified sine map

Let the Sine map $F(x_i) = \eta \sin(\pi x_i)$ be a seed map to Eq. (1), then the following map is obtained:

$$x_{i+1} = mod(a \cdot sc(b\eta \sin(\pi x_i)), N) \tag{12}$$

Modified sine sine map

If the Sine Sine map $F(x_i) = \sin(\pi\eta \sin(\pi x_i))$ is considered as a seed map to Eq. (1), then the following map is obtained:

$$x_{i+1} = mod(a \cdot sc(b \sin(\pi\eta \sin(\pi x_i))), N) \tag{13}$$

Modified cosine logistic map

Consider the Cosine Logistic map $F(x_i) = k \cos(rx_i(1 - x_i))$ as a seed map to Eq. (1), then a new modified map is obtained:

$$x_{i+1} = mod(a \cdot sc(bk \cos(rx_i(1 - x_i))), N) \tag{14}$$

PERFORMANCE EVALUATION

To evaluate the behavior of the new chaotic maps the following tools are used:

Phase diagrams

By projecting the inputs and outputs, phase diagrams can provide a qualitative portray of the behavior of chaotic maps. Irregularities in the phase diagram imply that the map's behavior is less predictable.

In Figs. 3, 4, 5, 6 the phase diagrams of the new chaotic maps and the phase diagrams of their corresponding seed maps are presented. It can be observed that while the shape of the seed maps' phase diagrams is distinguishable, the shape of the modified chaotic maps' phase diagram is indistinguishable. This means that the fixed points of the modified maps can not be obvious, contrary to the fixed points of the seed maps. As such, the task of predicting the parameters and states becomes considerably more difficult. Hence, the complexity of the new maps is higher.

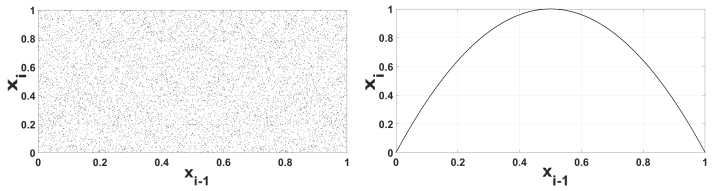

Figure 3 On the left the phase diagram of the modified Logistic map (11) is depicted, where $r = 4$, $a = 2 \cdot 10^6$, $b = 1$ and $N = 1$. On the right the phase diagram of the Logistic map, where $r = 4$.

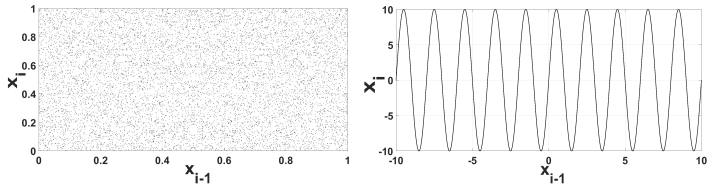

Figure 4 On the left the phase diagram of the modified sine map (12) is depicted, where $\eta = 10$, $a = 2 \cdot 10^6$, $b = 1$ and $N = 1$. On the right the phase diagram of the sine map, where $\eta = 10$.

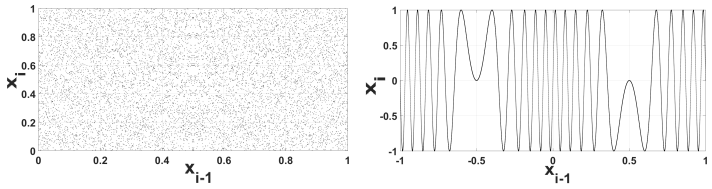

Figure 5 On the left the phase diagram of the modified sine sine map (13) is depicted, where $\eta = 10$, $a = 2 \cdot 10^6$, $b = 20$ and $N = 1$. On the right the phase diagram of the sine sine map, where $\eta = 10$.

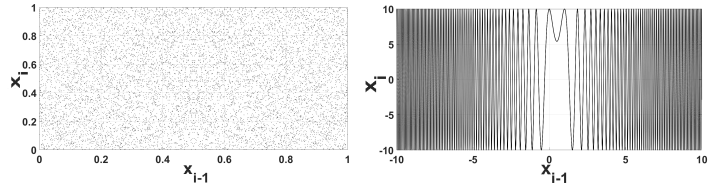

Figure 6 On the left the phase diagram of the modified cosine logistic map (14) is depicted, where $k = 10$, $a = 2 \cdot 10^6$, $b = 1$, $r = 4$ and $N = 1$. On the right the phase diagram of the cosine logistic map, where $k = 10$ and $r = 4$.

Bifurcation diagrams

By projecting the outputs with respect to the system's parameters, bifurcation diagrams shows the qualitative behavior of the system. Provides an insight on when, and the conditions under which the system enters or exits chaos.

From the comparison of the bifurcation diagrams in Figs. 7, 8, 9, 10 between the new maps and their classic counterparts, it can be seen that the enhanced maps exhibit larger regions of chaotic behavior, as well as the set of values is in the whole interval $[-1, 1]$. Therefore, it can be concluded that the modified maps exhibit more complicated behavior than their seed maps.

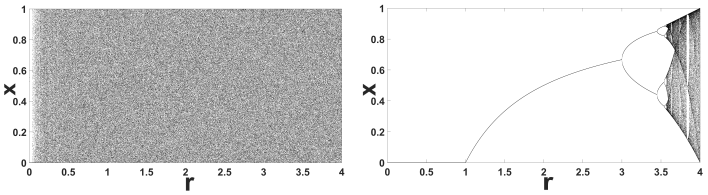

Figure 7 On the left the bifurcation diagram of the modified logistic map (11) with respect to r is depicted, where $a = 2 \cdot 10^6$, $b = 1$ and $N = 1$. On the right the bifurcation diagram of the Logistic map with respect to r.

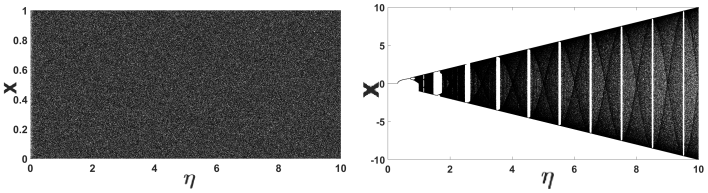

Figure 8 On the left the bifurcation diagram of the modified sine map (12) with respect to η is depicted, where $a = 2 \cdot 10^6$, $b = 1$ and $N = 1$. On the right the bifurcation diagram of the Sine map with respect to η.

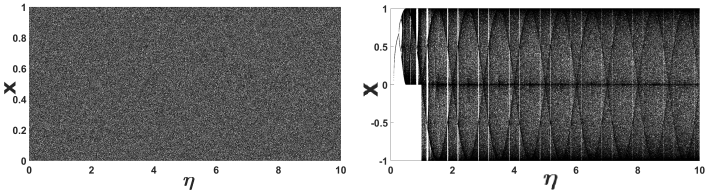

Figure 9 One the left the bifurcation diagram of the modified sine sine map (13) with respect to η is depicted, where $a = 2 \cdot 10^6$, $b = 20$ and $N = 1$. On the right the bifurcation diagram of the Sine Sine map with respect to η.

Lyapunov exponent diagrams

The Lyapunov exponent describes the average divergence of trajectories that begin from almost the same initial conditions. A positive Lyapunov exponent suggests that two neighboring trajectories in a dynamical system exponentially separate in each iteration, becoming different trajectories as time approaches infinity. As such, a positive Lyapunov exponent suggests chaos, and large Lyapunov exponent values indicate high complexity.

In Fig. 12, it can be seen that there exists a small region where the modified sine map (12) exhibits periodic behaviour. However, this is not visible to the corresponding bifurcation diagram

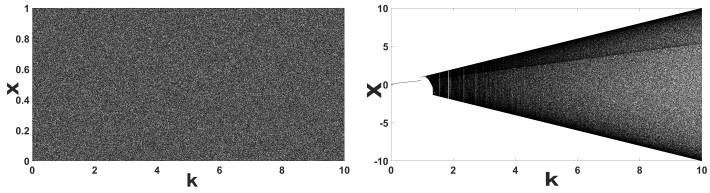

Figure 10 On the left the bifurcation diagram of the modified cosine logistic map (14) with respect to k is depicted, where $a = 2 \cdot 10^6$, $b = 1$, $r = 4$ and $N = 1$. On the right the bifurcation diagram of the cosine cogistic map with respect to k.

8, because the size of the region is much smaller than the overall interval in which the bifurcation diagram is plotted.

In addition, Figs. 11, 12, 13, 14 a comparison between the Lyapunov exponent diagrams of the modified chaotic maps and their original counterparts are presented. Immediately, from the high Lyapunov exponent values of the modified maps becomes apparent that they exhibit more complex behaviors than their seed maps.

Furthermore, from a first glance it seems that the modified maps mostly overcome chaos degradation, something very desirable in chaos based encryption. However, next it will be shown that this is not the case.

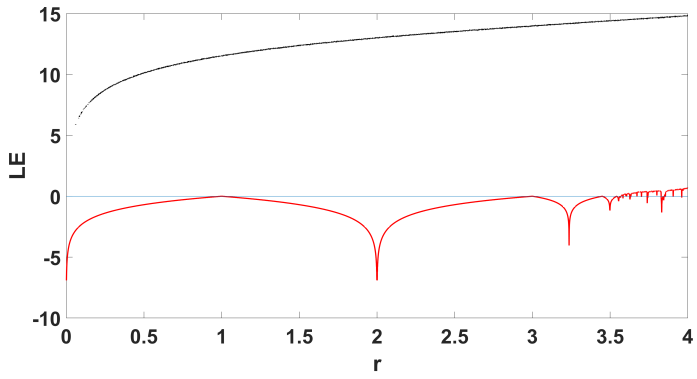

Figure 11 The Lyapunov exponent diagrams of the modified Logistic map (11) (black) and the Logistic map (red).

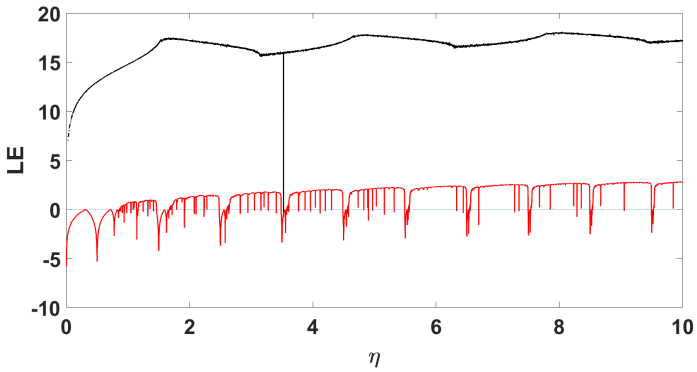

Figure 12 The Lyapunov exponent diagrams of the modified Sine map (12) (black) and the Sine map (red).

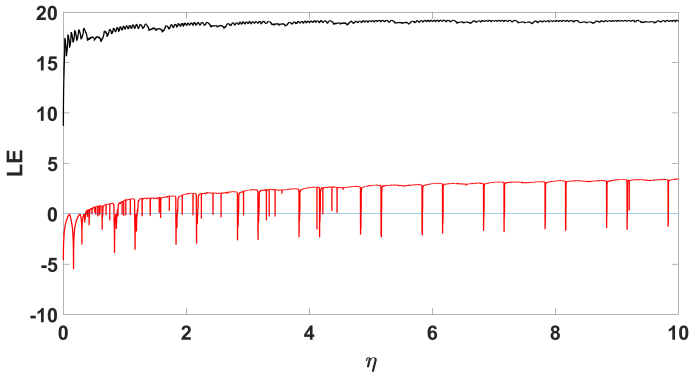

Figure 13 The Lyapunov exponent diagrams of the modified Sine Sine map (13) (black) and the Sine Sine map (red).

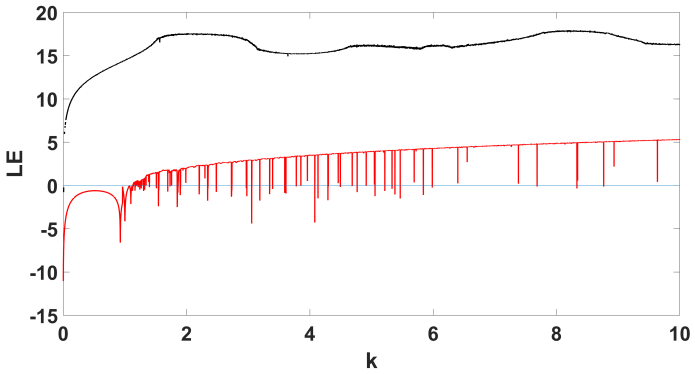

Figure 14 The Lyapunov exponent diagrams of the modified cosine logistic map (14) (black) and the cosine logistic map (red).

Fuzzy entropy

Like approximate, and sample entropy, fuzzy entropy is another measure to assess the complexity of a dynamical system based on fuzzy logic. High values of fuzzy entropy indicate high complexity. The reason for using fuzzy over sample entropy is because the complexity estimate is computed via the Gaussian function (Chen *et al.* 2009; Alawida *et al.* 2022; Dong *et al.* 2021),

$$\Theta(w_{i,j}^m, t) = \exp\{\frac{-(w_{i,j}^m)^2}{t}\} \tag{15}$$

where m is the embedding dimension which is set to 2, t is the tolerance value set to be $t = 0.15 * std(x)$, where $std(x)$ is the standard deviation of the time-series, and $w = \max_{(i,j)\in(0,m-1)} |x(i) - x(j)|$ the maximum distance between two sequences of length m.

In Figs. 15,17,19,21 a comparison of the fuzzy entropy values between the modified chaotic maps, and their classic counterparts is presented. It can be seen that the modified maps indeed display higher complexity than their counterparts. However, an undesirable effect in chaos cryptography that is not visible in the Lyapunov exponent diagrams depicted in Figs. 11, 12, 13, 14 becomes apparent, chaos degradation. This degradation in small periodic windows making it impossible to identify them in the bifurcation or Lyapunov exponent diagrams. Additionally, Fig. 17 verifies the periodic behavior of the modified sine map (12) presented in Fig. 12.

Furthermore, to investigate further these small periodic windows, and better understand the systems' behavior, the fuzzy entropy values were computed with respect to two parameters of the modified maps depicted in Figs. 16, 18, 20, 22. Again these diagrams verify that the modified chaotic maps exhibit a more complex behavior than their counterparts. However, the periodic windows, due to their size are not clearly visible in the diagrams.

Hence, despite the higher complexity of the new maps, a challenging problem is to modify the proposed chaotification technique in such way that chaos degradation is limited or absent.

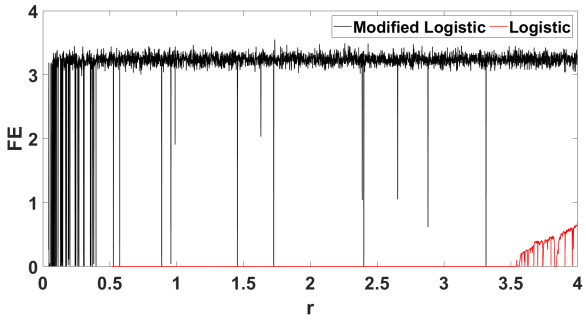

Figure 15 Fuzzy entropy comparison between the modified logistic map (11) with $a = 2 \cdot 10^6$, $b = 1$ and $x_0 = 0.1$, and the classic logistic map.

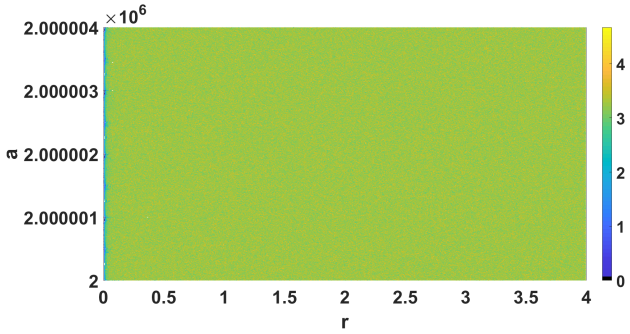

Figure 16 Fuzzy entropy of the modified logistic map (11) with respect to two parameters r, a with initial conditions $x_0 = 0.1$ and $b = 1$.

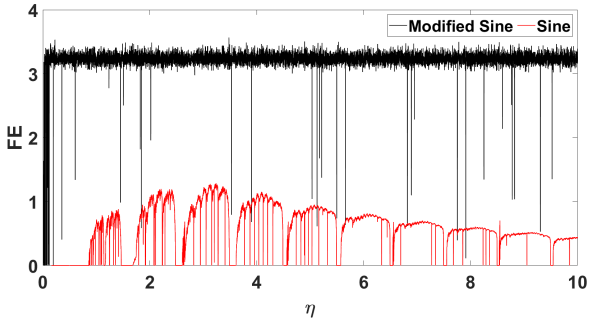

Figure 17 Fuzzy entropy comparison between the modified sine map (12) with $a = 2 \cdot 10^6$, $b = 1$ and $x_0 = 0.1$, and the classic sine map.

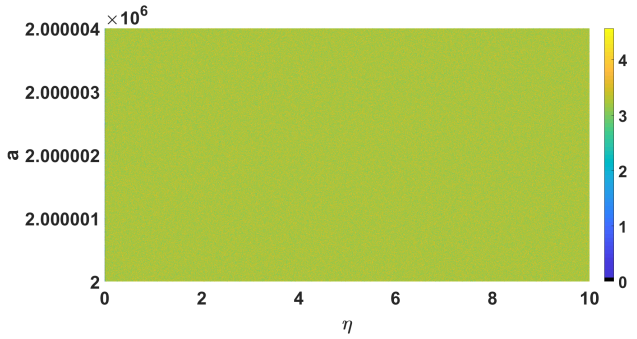

Figure 18 Fuzzy entropy of the modified sine map (12) with respect to two parameters η, a with initial conditions $x_0 = 0.1$ and $b = 1$.

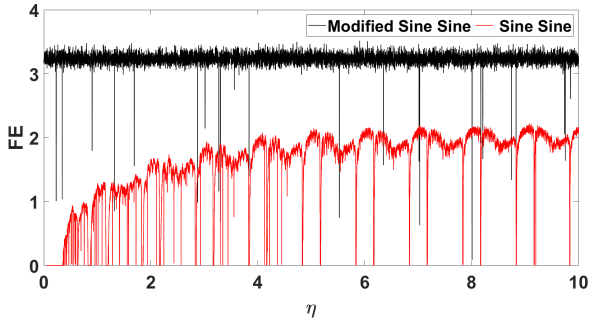

Figure 19 Fuzzy entropy comparison between the modified sine sine map (13) with $a = 2 \cdot 10^6$, $b = 20$ and $x_0 = 0.1$, and the classic sine sine map.

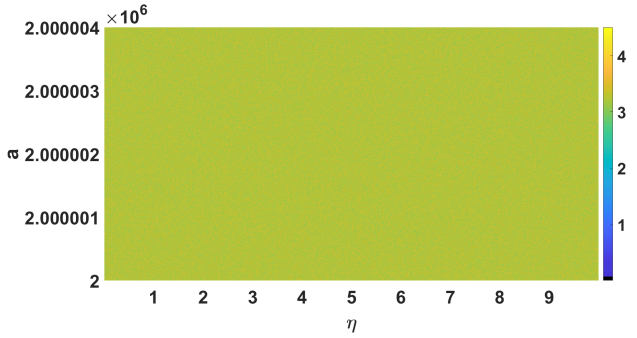

Figure 20 Fuzzy entropy of the modified sine sine map (13) with respect to two parameters η, a with initial conditions $x_0 = 0.1$ and $b = 20$.

ENCRYPTION OF SOUND SIGNAL

In this section the encryption of a sound signal is presented. The encryption consists of two parts, a sample shuffling, and a modulation of the source signal. The simulated signals are depicted in Fig. 23. As a source signal was used the poem *Three Things* by *Ella Wheeler Wilcox*. It can be downloaded by archive.org.

Step 1: A permutation to the source signal is performed. To do that consider two chaotic sequences of the form (11) with parameters (x_0, a_x, b_x, r_x) and (y_0, a_y, b_y, r_y) of same length as the samples of the source signal n. Consider also a sequence $z = \text{mod}\ (x + y, 1)$ with length n. Then, consider a vector $\mathcal{P}$ of length n, that takes its values in the interval $[1, n]$, applying the following

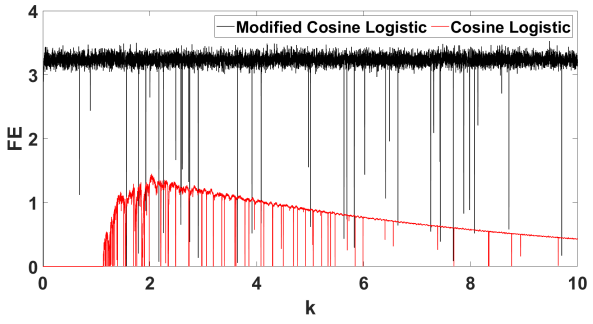

Figure 21 Fuzzy entropy comparison between the modified cosine logistic map (14) with $a = 2 \cdot 10^6$, $b = 1$, $r = 4$ and $x_0 = 0.1$, and the cosine logistic map with $r = 4$.

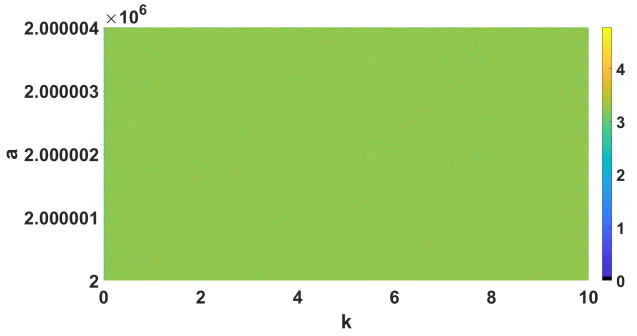

Figure 22 Fuzzy entropy of the modified cosine logistic map (14) with respect to two parameters k, a with initial conditions $x_0 = 0.1$ and parameter values $r = 4$ and $b = 1$.

rule, $p_i = \lceil \text{ mod } (10^{12} z_i, n) \rceil$ for $i = 1, \ldots, n$, where $\lceil \cdot \rceil$ is the ceiling operator. If $p_i = p_j$ for $i, j = 1, \ldots, n$, then p_j is rejected until all locations in the vector are unique. Then $\mathcal{P}$ provides the permutation order of the source signal. For example, let $p_1 = 200$, then the 1^{st} element of the source signal will move to the 200^{th} position. This is process is repeated until all elements in the source signal are repositioned and a new $\tilde{\mathcal{P}}$ signal is obtained.

Step 2: Then a modulation to the permuted signal is performed to obtain the final encrypted signal. To do that consider a chaotic sequence of any of the forms (11), (12), (13), (14) of length n. In this scenario it was chosen the chaotic map (11) with parameters (q_0, a_q, b_q, r_q). Finally, the encrypted signal is obtained by,

$$\mathcal{E} = \tilde{\mathcal{P}} + cos(\pi q).$$

Then the ciphered signal can be transmitted, and the receiver can reconstruct the original signal by solving

$$\tilde{\mathcal{P}} = \mathcal{E} - cos(\pi q)$$

and reversing step 1.

ENCRYPTION PERFORMANCE

A series of tests are run on the original, permuted, and encrypted signals to evaluate the performance of the encryption algorithm. Table 1 summarizes the results of the simulation performed in Matlab R2019a. The encryption key values are $x_0 = 0.2$, $y_0 = 0.8$, $q_0 = 0.1$, $a_x = 2 \cdot 10^6$, $a_y = 2 \cdot 10^6$, $a_q = 2 \cdot 10^6$, $b_x = 1$, $b_y = 1$, $b_q = 1$, $r_x = 3$, $r_y = 4$, $r_q = 5$.

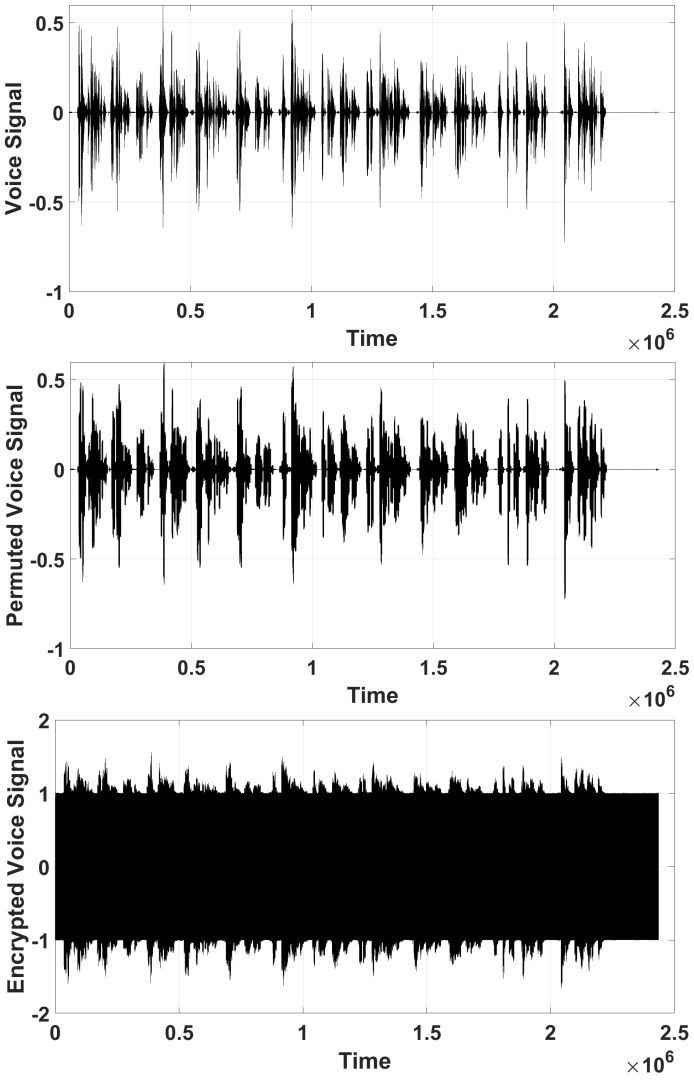

Figure 23 Original voice signal, permuted signal, and encrypted signal.

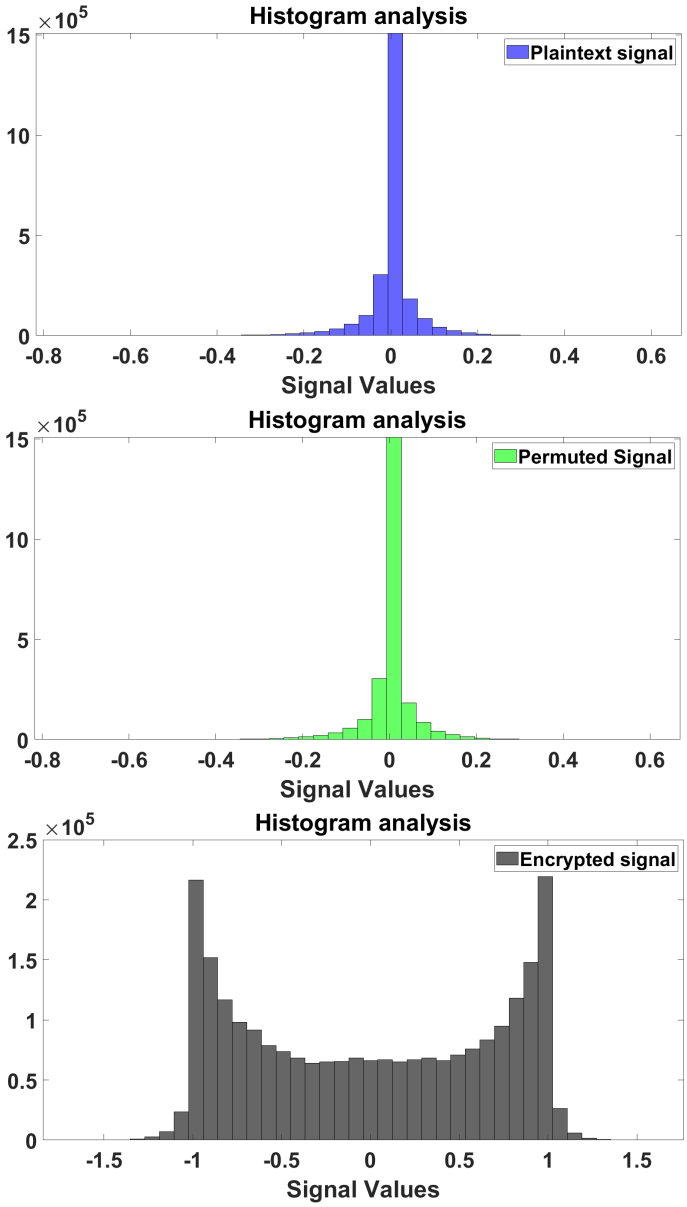

Figure 24 Histograms of the Original, Permuted, and Encrypted Signal.

Histogram

The original, permuted, and encrypted signal histograms are depicted in Fig. 24. As it can be observed contrary to the normal-like distributions of the original and permuted histograms, the encrypted signal exhibits a more complex histogram. As such, the hidden information is successfully masked. It should be noted that the original and permuted histograms are alike, since the values of the original signal were not altered but only shuffled.

Structural Similarity Index

The structural similarity (Algarni *et al.* 2021) between two signals is computed by,

$$SSIM = \frac{(2\mu_x\mu_y + S_1)(2cov(x,y) + S_2)}{(\mu_x^2 + \mu_y^2 + S_1)(var^2x + var^2y + S_2)} \tag{16}$$

where μ_x, μ_y the mean of the original and encrypted (or permuted) signals respectively, $varx$, $vary$ their variances, and $cov(x,y)$ their cross-covariance. It should be noted that S_1, S_2 are set to small values, in order to ensure stable results when the denominator is close to zero.

The structural similarity index value is in the interval $[-1,1]$, with 1 implying matched signals, and 0 when the signals have no similarity. Therefore, if the value is closing to zero, then the encryption is better. The structural similarity index between the original and the permuted signal is equal to 0.1253, and between the original and the encrypted signal is equal to 0.0019. Hence, since these values are close to zero, it can be concluded that the encryption is good.

Log-Likelihood Ratio

The Log-Likelihood Ratio estimates the encryption reliability (Elshamy *et al.* 2015). It assumes the segment can be depicted by a pth order all-pole linear predictive coding model,

$$x_i = \sum_{m=1}^{p} a_m x_{i-m} + G_x u_i \tag{17}$$

where x_i is the i^{th} signal sample, $a_m,\ m = 1, ..., p$ the coefficients of the all-pole filter, G_x is the filter gain, and u_i is an appropriate signal excitation input. Then the Log-Likelihood Ration is given by,

$$LLR = \left| \log \left(\frac{\mathbf{a}_x \mathbf{R}_y \mathbf{a}_x^T}{\mathbf{a}_y \mathbf{R}_z \mathbf{a}_y^T} \right) \right| \tag{18}$$

where $\mathbf{a}_x,\ \mathbf{a}_y$ the vectors of the Linear Prediction Coefficients of the form $[1\ a_1\ a_2\ \dots\ a_m]$ of the original signal, and the encrypted, or permuted signal respectively, and $\mathbf{R}_y$ the autocorrelation matrix of the encrypted or permuted signal. High Log-Likelihood Ratio values suggest a successful encryption. In order to short the computational time because the original signal is comprised by about 2.4 million samples, the original and encrypted (or permuted) signals were split to several segments, then the Log-Likelihood Ratio was computed as the mean value of the Log-Likelihood Ratio values of those segments. As such, the Log-Likelihood Ratio among the original and permuted signals is computed 2.5940 with variance 1.3347 and standard deviation 1.1553. Between the original and encrypted signals the Log-Likelihood Ration is 2.5930 with variance 1.3419 and standard deviation 1.1584. Since the values are both high, it can be concluded that the encryption is successful.

Signal to Noise Ration

The signal-to-noise ratio is another metric used to assess the quality of an encryption (Mosa *et al.* 2011). The signal-to-noise ratio is given by,

$$SNR = 10 \log_{10} \frac{\sum_{i=1}^{N} x_i^2}{\sum_{i=1}^{N} (x_i - y_i)^2} \tag{19}$$

where x, y are the original and encrypted (or permuted, decrypted) signals respectively. High positive signal-to-noise ratio value indicate strong relation between the two signals, while low negative signal-to-noise ratio value imply mismatch between the signals. The signal-to-noise ratio among the original and the decrypted signals is 306.8672. Therefore, indicating that the decryption is successful. The signal-to-noise ratio between the original and permuted signals is -3.0148, and among the original and encrypted signals is -21.6418. Hence, also from this measure it can be deduced that the encryption is good.

Correlation Coefficient

The correlation coefficient (Renza *et al.* 2019; Algarni *et al.* 2021) among two signals is given by,

$$r_{xy} = \frac{cov(x, y)}{\sqrt{var(x)}\sqrt{var(y)}} \tag{20}$$

where $cov(x, y)$ is the covariance of the two signals and $var(x), var(y)$ their variances. The correlation coefficient takes its values in the interval $[0, 1]$. When the value is close to zero means that the two signals are uncorrelated. The correlation coefficient between the original and the permuted signal is -0.0010, between the original and the encrypted signal is -0.00047, in both of these cases is implied uncorrelated signals, while the correlation coefficient between the original and the decrypted signal is 1, and that is because they are identical, as it should.

Spectral Distortion

The spectral distortion is the measure to quantify the mismatch between two signals (Renza *et al.* 2019). Therefore, spectral distortion can be used to compare the original sound with the permuted, encrypted, and the decrypted sounds. It is given by,

$$SD = \frac{1}{N} \sum_{i=0}^{N-1} |V_{x,i} - V_{y,i}| \tag{21}$$

where $V_{x,i}, V_{y,i}$ are the spectrum of the signals in decibels at any given point in time i. When the spectral distortion value is high, a higher difference between the two signals is implied, and when the spectral distortion value is equal to zero the two signals are matched. As such, large values of spectral distortion are indicative of a good encryption, and zero or close to zero value implies successful decryption. The spectral distortion among the original and permuted signals is 29.3021, between the original and encrypted signals is 36.7113, and among the original and decrypted signals is $3.7596 \cdot 10^{-12} \approx 0$. Hence, it can be deduced that the encryption is good as well that the decryption is successful.

Approximate Entropy

The approximate entropy proposed in (Pincus 1991) provides an indication for the complexity of a time series. The higher the approximate entropy of a time series, the more complex it is considered (Liu *et al.* 2021). As a result, the approximate entropy value of the encrypted signal must be greater than that of the original. The approximate entropy of the original signal is 0.6235, 1.9402 after the permutation is performed, and 1.9696 for the encrypted one, indicating that the encrypted signal has the highest approximate entropy. It should be noted that the original, permuted, and encrypted signals were divided into several sub-signals for computational reasons, and their approximate entropy is computed as the mean approximate entropy of those sub-signals. The variance for each signal is 0.2453, 0.0561, and 0.0011, and the standard deviation is 0.4953, 0.2369, and 0.0342 respectively.

Key space and Sensitivity

Every encryption system must be robust to brute force attacks. This requires that the key space be higher than 2^{100} (Alvarez and Li 2006). Three chaotic maps (11) are used in the proposed encryption system, with parameters (x_0, a_x, b_x, r_x), (y_0, a_y, b_y, r_y) and (q_0, a_q, b_q, r_q), given that for this map the parameter b is set to be always 1. As a result, the system has 9 parameters. For a precision of 16 digits, the upper bound for the key space is computed as $10^{9 \cdot 16} = 10^{144} = (10^3)^{48} \approx (2^{10})^{48} = 2^{480}$. Note, that since the map (11) exhibits periodic windows in very small regions with respect to its control parameters the actual key space is less than 2^{480}. However, the requirement to resist brute force attacks is still met.

Moreover, since this encryption system is chaos-based, any minor change in the parameter values will result in a flawed decryption process. As a result, any encrypted signal can only be decrypted by the receiver only as long as the given keys are precisely known.

Table 1 Performance of the encryption scheme

Signals	Original Sound	Permuted Sound	Encrypted Sound	Decrypted Sound
Structural Similarity Index	-	0.1253	0.0019	1
Log-Likelihood Ratio	-	2.5940	2.5930	-
Signal Noise Ratio	-	−3.0148	−21.6418	306.8672
Correlation Coefficient	-	−0.0010	−0.00047	1
Spectral Distortion	0	29.3021	36.7113	$3.7596 \cdot 10^{-12}$
Approximate Entropy	0.6235	1.9402	1.9696	0.6235

CONCLUSION

In this work, a new chaotification method is proposed by using a double nonlinear transformation based on the modulo operator and secant function to enhance the chaotic behavior and complexity of existing chaotic maps. The theoretical analysis based on the Lyapunov exponent revealed that for a given seed map applied on the proposed chaotification model, the modified map can achieve higher Lyapunov exponent values than the original map. As a result, the proposed chaotification technique can enlarge the chaotic region of a one-dimensional chaotic map while also improving its dynamic properties. To validate this theoretical result, numerical experiments were applied using as seed maps, the logistic, sine, sine sine, and the cosine logistic maps, through well-known tools for studying the dynamical behavior of chaotic systems, namely the phase diagrams, bifurcation diagrams, Lyapunov exponent diagrams, and the fuzzy entropy. From these experiments it was shown that indeed the modified maps exhibit larger chaotic regions, higher lyapunov exponents, indistinguishable phase diagrams. Therefore, the chaotification technique improves the dynamic properties of the seed maps. However, the fuzzy entropy showed chaos degradation in the new maps which is in the form of small periodic windows. These periodic windows are not a desirable property, especially in chaos based encryption. As such, a modification of the chaotification technique must be considered. A possible modification which will be studied is as follows:

$$x_{i+1} = \mod\left(a \cdot \frac{1}{(b\cos(F(x_i)) + c)}, N\right)$$

where parameter c is small in order to guarantee consistent performance when the denominator is close to zero.

Moreover, to illustrate a practical application of the proposed chaotification model, a voice encryption scheme was designed. The system is based on a permutation, and a modulation process both derived by the modified logistic map 11. A variety of tests and measures were used to showcase that the resulting encrypted signal is both random and secure.

Furthermore, for future research the implementation of this proposed encryption scheme on digital hardware, such as ARM processors, FPGA, and microcontrollers will be considered. When it comes to digital implementation of chaos-based cryptography techniques, the problem of chaotic map reproducibility from one device to another arises. Given the nonlinear nature of the maps, computational accuracy is of the utmost importance. One round-off error in the least significant digits can lead to completely different trajectories throughout various devices even with exact initial conditions and control parameter values (Teh *et al.* 2020; Sayed *et al.* 2020). Therefore, the output replication problem across different devices becomes apparent. In addition, an investigation of the increased computational effort by the modulo operator and the secant function in comparison to the classic maps is of interest.

Finally, it is intended to extent our results to multidimensional chaotic maps, and construct new hyperchaotic systems.

Availability of data and material

Not applicable.

Conflicts of interest

The authors declare that there is no conflict of interest regarding the publication of this paper.

LITERATURE CITED

Abd, M. H., G. A. Al-Suhail, F. R. Tahir, A. M. Ali Ali, H. A. Abbood, *et al.*, 2022 Synchronization of monostatic radar using a time-delayed chaos-based fm waveform. Remote Sensing **14**: 1984.

Ablay, G., 2022 Lyapunov exponent enhancement in chaotic maps with uniform distribution modulo one transformation. Chaos Theory and Applications **4**: 45–58.

Adeyemi, V.-A., E. Tlelo-Cuautle, F.-J. Perez-Pinal, and J.-C. Nuñez-Perez, 2022 Optimizing the maximum lyapunov exponent of fractional order chaotic spherical system by evolutionary algorithms. Fractal and Fractional **6**: 448.

Alawida, M., J. S. Teh, A. Mehmood, A. Shoufan, *et al.*, 2022 A chaos-based block cipher based on an enhanced logistic map and simultaneous confusion-diffusion operations. Journal of King Saud University-Computer and Information Sciences .

Algarni, A. D., N. F. Soliman, H. A. Abdallah, A. El-Samie, and E. Fathi, 2021 Encryption of ecg signals for telemedicine applications. Multimedia Tools and Applications **80**: 10679–10703.

Alvarez, G. and S. Li, 2006 Some basic cryptographic requirements for chaos-based cryptosystems. International journal of bifurcation and chaos **16**: 2129–2151.

Borah, M., A. Gayan, J. S. Sharma, Y. Chen, Z. Wei, *et al.*, 2022 Is fractional-order chaos theory the new tool to model chaotic pandemics as covid-19? Nonlinear Dynamics pp. 1–29.

Bovy, J., 2004 Lyapunov exponents and strange attractors in discrete and continuous dynamical systems. Theoretica Phys. Project, Catholic Univ. Leuven, Flanders, Belgium, Tech. Rep **9**: 1–19.

Chen, W., J. Zhuang, W. Yu, and Z. Wang, 2009 Measuring complexity using fuzzyen, apen, and sampen. Medical engineering & physics **31**: 61–68.

de la Fraga, L. G., E. Tlelo-Cuautle, V. Carbajal-Gómez, and J. Munoz-Pacheco, 2012 On maximizing positive lyapunov exponents in a chaotic oscillator with heuristics. Revista mexicana de física **58**: 274–281.

Dong, C., K. Rajagopal, S. He, S. Jafari, and K. Sun, 2021 Chaotification of sine-series maps based on the internal perturbation model. Results in Physics **31**: 105010.

Elshamy, E. M., E.-S. M. El-Rabaie, O. S. Faragallah, O. A. Elshakankiry, A. El-Samie, *et al.*, 2015 Efficient audio cryptosystem based on chaotic maps and double random phase encoding. International Journal of Speech Technology **18**: 619–631.

Fadil, E., A. Abass, and S. Tahhan, 2022 Secure wdm-free space optical communication system based optical chaotic. Optical and Quantum Electronics **54**: 1–14.

Grassi, G., 2021 Chaos in the real world: Recent applications to communications, computing, distributed sensing, robotic motion, bio-impedance modelling and encryption systems. Symmetry **13**: 2151.

Hua, Z., B. Zhou, and Y. Zhou, 2018 Sine chaotification model for enhancing chaos and its hardware implementation. IEEE Transactions on Industrial Electronics **66**: 1273–1284.

Li, Y., X. He, and D. Xia, 2021 A chaotification model based on sine and cosecant functions for enhancing chaos. Modern Physics Letters B **35**: 2150258.

Liu, L., H. Xiang, and X. Li, 2021 A novel perturbation method to reduce the dynamical degradation of digital chaotic maps. Nonlinear Dynamics **103**: 1099–1115.

Mammedov, Y. D., E. U. Olugu, and G. A. Farah, 2022 Weather forecasting based on data-driven and physics-informed reservoir computing models. Environmental Science and Pollution Research **29**: 24131–24144.

Mosa, E., N. W. Messiha, O. Zahran, A. El-Samie, and E. Fathi, 2011 Chaotic encryption of speech signals. International Journal of Speech Technology **14**: 285–296.

Moysis, L., D. N. Butusov, A. Tutueva, V. Ostrovskii, I. Kafetzis, *et al.*, 2022a Introducing chaos and chaos based encryption applications to university students-case report of a seminar. In *2022 11th International Conference on Modern Circuits and Systems Technologies (MOCAST)*, pp. 1–6, IEEE.

Moysis, L., I. Kafetzis, M. S. Baptista, and C. Volos, 2022b Chaotification of one-dimensional maps based on remainder operator addition. Mathematics **10**: 2801.

Nagashima, H., Y. Baba, and M. Nakahara, 2019 *Introduction to chaos: physics and mathematics of chaotic phenomena*. CRC Press.

Natiq, H., S. Banerjee, and M. Said, 2019 Cosine chaotification technique to enhance chaos and complexity of discrete systems. The European Physical Journal Special Topics **228**: 185–194.

Petavratzis, E., C. Volos, L. Moysis, H. Nistazakis, A. Giakoumis, *et al.*, 2022 Experimental coverage performance of a chaotic autonomous mobile robot. In *2022 11th International Conference on Modern Circuits and Systems Technologies (MOCAST)*, pp. 1–4, IEEE.

Pincus, S. M., 1991 Approximate entropy as a measure of system complexity. Proceedings of the National Academy of Sciences **88**: 2297–2301.

Renza, D., S. Mendoza, *et al.*, 2019 High-uncertainty audio signal encryption based on the collatz conjecture. Journal of Information Security and Applications **46**: 62–69.

Sayed, W. S., A. G. Radwan, H. A. Fahmy, and A. El-Sedeek, 2020 Software and hardware implementation sensitivity of chaotic systems and impact on encryption applications. Circuits, Systems, and Signal Processing **39**: 5638–5655.

Shahi, S., F. H. Fenton, and E. M. Cherry, 2022 Prediction of chaotic time series using recurrent neural networks and reservoir computing techniques: A comparative study. Machine Learning with Applications **8**: 100300.

Teh, J. S., M. Alawida, and Y. C. Sii, 2020 Implementation and practical problems of chaos-based cryptography revisited. Journal of Information Security and Applications **50**: 102421.

Wang, B., J. Liu, M. O. Alassafi, F. E. Alsaadi, H. Jahanshahi, *et al.*, 2022 Intelligent parameter identification and prediction of variable time fractional derivative and application in a symmetric chaotic financial system. Chaos, Solitons & Fractals **154**: 111590.

Wu, Q., 2021 Cascade-sine chaotification model for producing chaos. Nonlinear Dynamics **106**: 2607–2620.

Xiu, C., J. Fang, and X. Ma, 2022 Design and circuit implementations of multimemristive hyperchaotic system. Chaos, Solitons & Fractals **161**: 112409.

Zeraoulia, E., 2012 *Robust chaos and its applications*, volume 79. World Scientific.

Zhang, Z., H. Zhu, P. Ban, Y. Wang, and L. Y. Y. Zhang, 2022 Buffeting chaotification model for enhancing chaos and its hardware implementation. IEEE Transactions on Industrial Electronics .

How to cite this article: Charalampidis, N., Volos, C., Moysis, L., and Stouboulos, I. A Chaotification Model Based on Modulo Operator and Secant Functions for Enhancing Chaos. *Chaos Theory and Applications*, 4(4), 274-284, 2022.