Applied Mathematics & Information Sciences
An International Journal

http://dx.doi.org/10.12785/amis/090650

Encryption Applications of a Generalized Chaotic Map

Salwa K. Abd-El-Hafiz, Ahmed G. Radwan[*] *and Sherif H. AbdEl-Haleem*

Engineering Mathematics Department, Faculty of Engieering, Cairo University, Giza 12613, Egypt

Received: 12 Mar. 2015, Revised: 10 May 2015, Accepted: 11 May 2015
Published online: 1 Nov. 2015

Abstract: This paper presents the mathematical aspects of a generalized Sine map with arbitrary powers and scaling factor. The added parameters increase the degrees of freedom of the Sine map and give a versatile response that can be utilized in many applications. For each added parameter, the map's chaotic behavior is analyzed using fixed points, bifurcation diagrams and Lyapunov exponents. Furthermore, two image encryption applications are introduced based on the generalized Sine map. The first system only performs pixel-value substitutions to focus on the effect of utilizing the generalized map. This system is controlled by fifteen different parameters and initial conditions of three generalized Sine maps.The second system performs both permutations and substitutions to achieve Shannon's diffusion and confusion properties. The two systems are analyzed using miscellaneous evaluation criteria such as pixel correlation coefficients, differential attack measures, histogram distributions and the National Institute of Standards and Technology (NIST) statistical test suite. Key sensitivity analysis is also performed and the mean square error and entropy measures are calculated. The analysis results are promising and demonstrate the benefits of utilizing the designed generalized map in image encryption applications.

Keywords: Cryptography, discrete time chaotic systems, image encryption, sine map

1 Introduction

Since the 1930's, chaotic systems have been used in the modeling and processing activities of miscellaneous areas of science [1,2]. Such areas include biology [3], medicine [4], business [5], computer science [6,7], physics and chemistry [8]. In engineering and communication, chaotic dynamics have also been extensively utilized. Some approaches design new chaotic generators based on analog [9], digital [10] or mixed circuits [11]. Other approaches utilize classical or new designs of discrete chaotic systems. For example, the well-known logistic map is extensively utilized in secure communication and image encryption (refer for example to [12] and [13]). In addition, some pseudorandom number generators utilize different discrete-time chaotic circuits (e.g., [14,15]).

Chaos-based cryptography has been used for more than two decades and numerous chaotic systems have been utilized in text, image, sound or video encryption. In order to fulfill some basic cryptographic requirements, Alvarez and Li provide guidelines to be followed when designing a new chaos-based cryptosystem [16]. The utilized chaotic systems include discrete maps, continuous attractors, fractional-order attractors, or fractals [17,18,19,20,21]. For instance, [17] uses the fractional-order Lorenz attractor in image encryption. In [18], a color image encryption scheme is designed based on coupled 3D continuous chaotic systems and a secure hash algorithm is employed to generate one-time keys dependent on the plain image. On the other hand, Tong and Cui design a new 2D chaotic function by exploiting two 1D chaotic functions which switch randomly [19]. Their image encryption scheme uses the new 2D chaotic function, image pixel permutation and 3D baker scheme. In addition, Zhang *et al.* [20] utilize the characteristics of bit-level operations and the intrinsic bit features of the image in an expand-and-shrink strategy that shuffles the image with reconstructed permuting plane. Fractals are also used as the stream, or medium, for encrypting images by combining ideas from symmetric-key stream cryptography and spatial domain steganography [21].

Despite the fact that the logistic map is widely used in encryption, many approaches introduce new chaotic maps or enhance and combine existing ones in order to improve security and performance (e.g., [22,23,24]). In [22], a new hybrid chaotic map, which is constructed by composition of the logistic map, Henon map and Ikeda map, reveals remarkable sensitivity to initial condition and parameters. On the other hand, Chen *et. al* [23] use multiple chaotic dynamics and two chaotic maps are required in their cryptosystem.One map encrypts the first

[*] Corresponding author e-mail: agradwan@ieee.org

plaintext block and, then, the other map encrypts the next plaintext block using final output of the first map as initial value. Pisarchik and Zanin [24] also presented a cryptosystem for direct encryption of color images, based on chaotically coupled chaotic maps. Their proposed cipher provides good confusion and diffusion properties because of the chaotic mixing of pixels'colors.

The classification, bifurcation, and similarities of iterated maps can be explained by the mathematical theory on one-dimensional maps [25]. According to the Sarkovskii theorem [26], if the function has a periodic point of period three then chaos can be achieved at a certain range of the control parameter. The conventional Sine map is defined by $x_{n+1} = r\sin(\pi x_n)$, where r, $x \in \mathbb{R}$. This map generates a bifurcation diagram that is symmetric with respect to both axes of the r-x plane. Figure 1(a) shows this bifurcation diagram for $r \in [-\pi,\pi]$. By keeping r and x in the interval $[0,1]$, the map is restricted to the first quadrant as shown in Fig. 1(b). The conventional Sine map depends on a single parameter r, which limits the map's behavior and applications.

This paper introduces a generalized Sine map where the conventional map is considered as a special case. The added parameters, which are arbitrary powers and scaling factor, increase the degrees of freedom of the map and produce a versatile response that can be utilized in many applications. The generalized Sine map is described by

$$x_{n+1} = f(x_n,r,\gamma,\beta,\alpha) = r\sin^{\gamma}(\alpha\pi x_n^{\beta}), \qquad (1)$$

where α,β, and γ are real parameters greater than zero. The new generalized one-dimensional Sine map has four parameters (r,γ,β,α).

To analyze the effect of each of the newly added parameters on the Sine map's chaotic behavior, three special cases are discussed. In each of the three special cases, r and one of the newly introduced parameters (γ,β,α) are varied while the other two are set to unity. In addition to the presentation and discussion of the generalized Sine map, this paper utilizes it in an image encryption application which demonstrates the advantage of the added degrees of freedom. It should be mentioned that generalized logistic and tent families have been recently investigated in [27,28,29].

Sections 2 to 4 of this paper provide detailed analysis of the chaotic behavior of the Sine map due to the three parameters γ, β and α, respectively. In this analysis, fixed points, bifurcation diagrams and maximum Lyapunov exponents are discussed. Section 5 presents two image encryption applications based on the generalized Sine map, which give promising results. Finally, conclusions and future work are provided in Section 6.

2 Chaotic Behavior When $\gamma \neq 1$ and $\alpha = \beta = 1$

Assuming that $f(x,r,\gamma) = r\sin^{\gamma}(\pi x)$, then the peak of this function equals r and it exists at $x = x_p = 0.5$. To ensure the closure property of $x \in [0,1]$, $r \in [0,1]$ in all cases independent of γ. Figure 2 shows the projection of the fifth iteration f^5 in the x-γ plane for different values of r. As r increases, values of the fifth iteration increase up to almost the full range, when $r = 1.0$. As γ increases, the peaks increase in number and get deformed with different rotations as evident from Fig. 2 when $r = 0.9$ and $r = 1.0$.

2.1 Nontrivial Fixed Points

Figure 3 plots $f(x,r,\gamma)$ versus x for different values of r and γ. This figure indicates the expected number and location of the fixed points, x_*. For $\gamma < 1$, only one nontrivial fixed point can exist. This fixed point, x_*, is less than $x_p = 0.5$ when $r < 0.5$ and is greater than x_p when $r > 0.5$. For $\gamma > 1$, there can be zero, one, or two nontrivial fixed points depending on the values of γ and r. Given this qualitative information, the fixed points can be numerically calculated for different values of the parameters r and γ from:

$$x_* = f(x_*,r,\gamma) = r\sin^{\gamma}(\pi x_*). \qquad (2)$$

Figure 4 shows the values of the fixed points, x_*, and the derivative $f'(x_*,r,\gamma)$ at those fixed points. For $\gamma \leq 1$, Fig. 4 shows the nontrivial solutions where x_* increases as r increases. In addition, the nonlinearity of the curve x_* increases as γ increases. The stability of the fixed points is determined based on the derivative of $f(x_*,r,\gamma)$. Hence, Fig. 4 also shows the values of $f'(x_*,r,\gamma)$ for different values of r and γ. If $|f'(x_*,r,\gamma)| < 1$, then the fixed point is stable (i.e., sink). If $|f'(x_*,r,\gamma)| > 1$, then the fixed point is unstable (i.e., source).

When $\gamma = 0.1$, the system has a single fixed point in the full range of r and it is always stable. However, as γ increases the absolute derivative at the fixed point begins to decrease below -1 as r increases. Therefore, there are critical points (r_b, x_{*b}) at which this derivative absolute value becomes unity as follows:

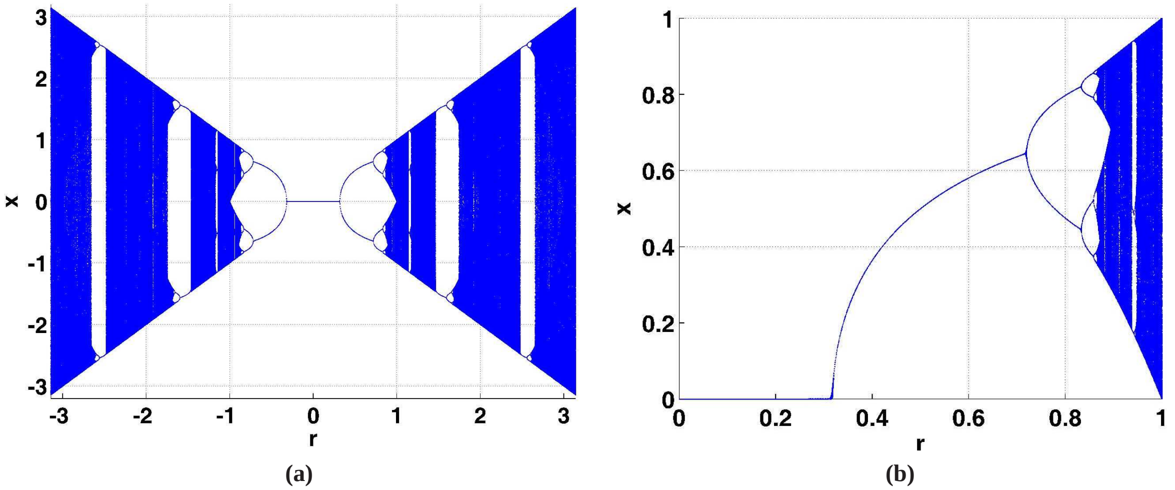
$$f'(x_{*b},r_b,\gamma) = \pm 1 = \pi r_b \gamma \sin^{\gamma-1}(\pi x_{*b})\cos(\pi x_{*b}). \qquad (3)$$

By substituting $r_b = \frac{x_{*b}}{\sin^{\gamma}(\pi x_{*b})}$ from (2) into (3), the flip bifurcation point (r_b, x_{*b}) in the region $[0,1]\times[0,1]$ occurs when $f'(x_{*b},r_b,\gamma) = -1$. Hence, $x_{*b} \in [0,1]$ is obtained from the following equation:

$$\pi\gamma x_{*b} + \tan(\pi x_{*b}) = 0. \qquad (4)$$

Consequently, the equation of the bifurcation curve is:

$$r_b = x_{*b}(\sin(\pi x_{*b}))^{\frac{\tan(\pi x_{*b})}{\pi x_{*b}}}. \qquad (5)$$



(a) (b)

Fig. 1: Sine bifurcation diagrams when (a) $r, x \in [-\pi, \pi]$ and (b) $r, x \in [0, 1]$.

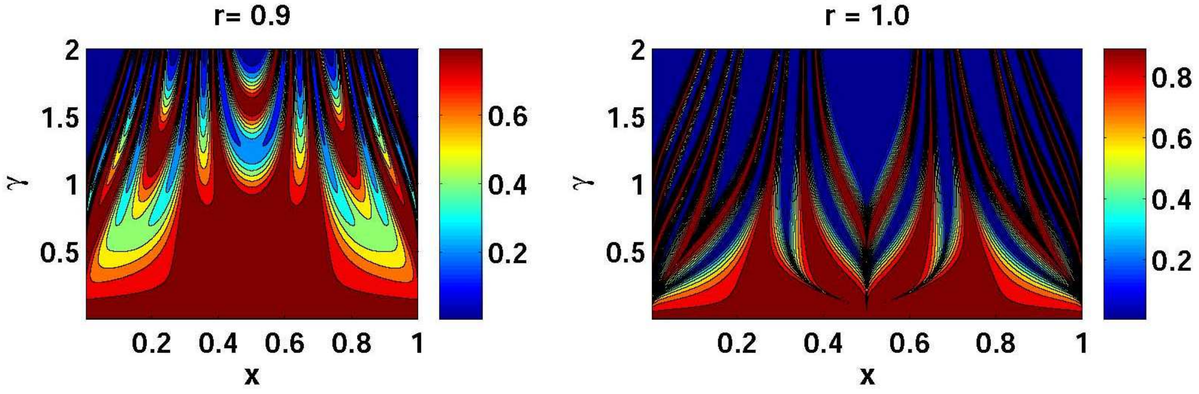
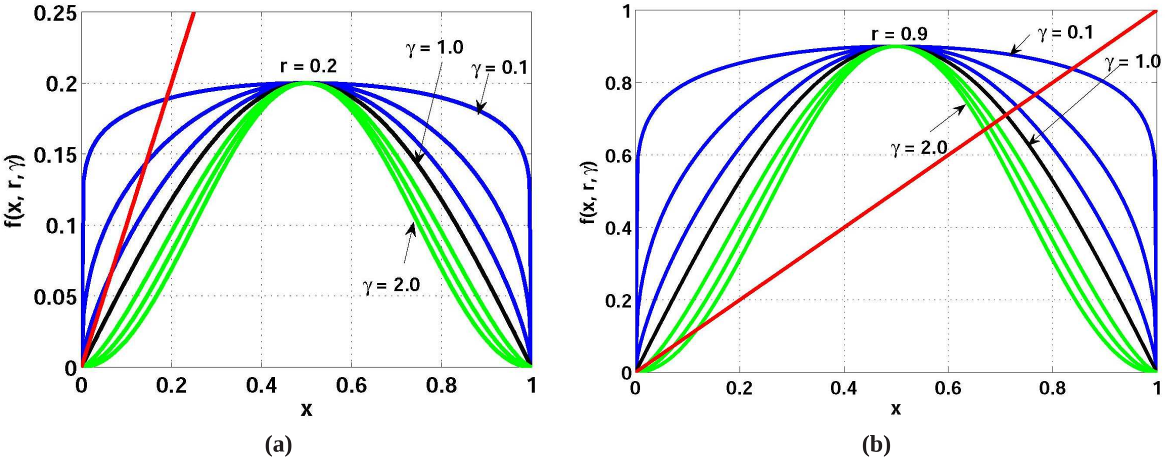


Fig. 2: Projection of the function iteration f^5 in the x-γ plane for different values of r.



(a) (b)

Fig. 3: Expected fixed points of $f(x, r, \gamma) = r\sin^{\gamma}(\pi x)$ for different values of r and γ (a) $r = 0.2$ and (b) $r = 0.9$.

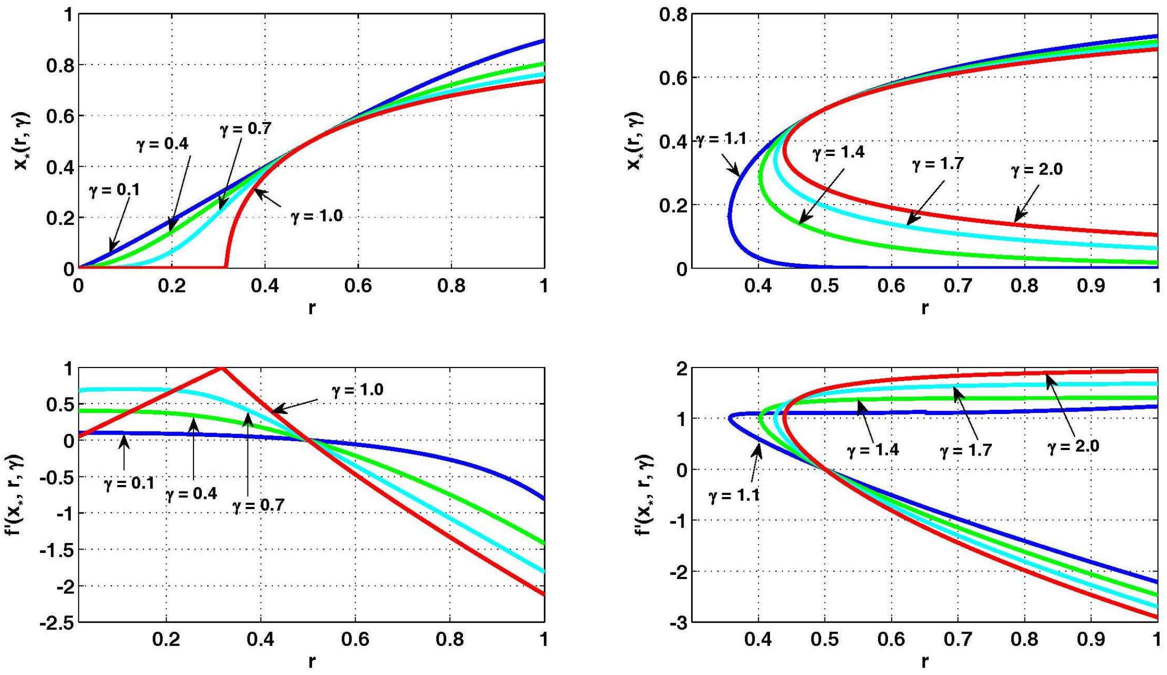


Fig. 4: Fixed points and derivatives of $f(x,r,\gamma) = r\sin^{\gamma}(\pi x)$ for different values of γ.

For $\gamma > 1$, Fig. 3 and Fig. 4 show that there are no nontrivial fixed points for small values of r. As r increases, there is a fold bifurcation point (r_s, x_{*s}) at which the nontrivial fixed-points start to appear. When $r > r_s$ and based on the fixed point stability criteria discussed in [30] , two fixed-points occur. One of the fixed points is always unstable ($f' > 1$) and the other remains stable until f' reaches -1 (i.e., it is stable as long as $|f'| < 1$).

The fold bifurcation point (r_s, x_{*s}) is obtained by solving $f'(x_*, r, \gamma) = 1$ to get

$$\pi\gamma x_{*s} - \tan(\pi x_{*s}) = 0. \qquad (6)$$

It is also at the location where the peak in the r-x_* curve occurs $\left(\frac{\partial r}{\partial x_*}|_{x_*=x_{*s}} = 0\right)$ (see Fig. 4) [25]. The following flip bifurcation point (r_b, x_{*b}) occurs when $f'(x_{*b}, r_b, \gamma) = -1$ similar to the case when $\gamma \leq 1$.

Figure 5 plots the fold bifurcation points (r_s, x_{*s}), which indicate the onset of nontrivial fixed points. It also plots the following period-two flip bifurcation points (r_b, x_{*b}). As long as $x_{*s} = 0$, the bifurcation diagram is continuous and when $x_{*s} > 0$ the bifurcation diagram suffers from discontinuity. From Fig. 5(a), it is clear that the bifurcation diagram is continuous when $\gamma \leq 1$ and suffers from discontinuity when $\gamma > 1$. In addition, since the parameter r is restricted to $r \in [0,1]$, Fig. 5(b) shows that there is no bifurcation at all when $\gamma < \gamma_{th} = 0.17$. It should also be noted that Fig. 5(b) demonstrates that the value of r_s increases as γ increases.

The values of the bifurcation points given in Fig. 5 are in accordance with the bifurcation diagrams given in Fig. 6. In Fig. 6(a), $\gamma < \gamma_{th} = 0.17$ and there is no bifurcation at all. In Figs. 6(b) and 6(c), $\gamma_{th} \leq \gamma \leq 1$ and $x_{*s} = 0$. Hence, the bifurcation diagram is continuous and the nontrivial fixed points start from the corresponding r_s given in Fig. 5(b). For $\gamma = 1$, nontrivial fixed-points start to occur when $f' = 1$ at $r_s = 1/\pi$ and $x_{*s} = 0$ and, therefore, the bifurcation diagram is still continuous (refer to Fig. 1(b)). In Fig. 6(d), $\gamma > 1$ and there is a discontinuity in the bifurcation diagram because of the nonzero x_{*s}.

2.2 Bifurcation Diagrams

From the previous analysis, the bifurcation diagram of the proposed map depends on some critical values as shown in Fig. 5. Figure 6(a-d) illustrate the differences and progress of the diagram versus $r \in [0,1]$ as γ increases from 0.1 to 1.5. As explained in Section 2.1, there is a single stable fixed point and no bifurcation occurs at $\gamma = 0.1$. As γ increases beyond γ_{th}, the first flip bifurcation (period two) occurs at the points (r_b, x_{*b}), which are given in Fig. 5. The bifurcation diagram suffers from discontinuities once the parameter γ exceeds 1. Figure 6(d) shows that two supplementary fixed points are caused by the fold bifurcation at (r_s, x_{*s}) and, then, the flip bifurcation occurs at (r_b, x_{*b}) given in Fig. 5. In addition, the bifurcation diagram changes considerably by

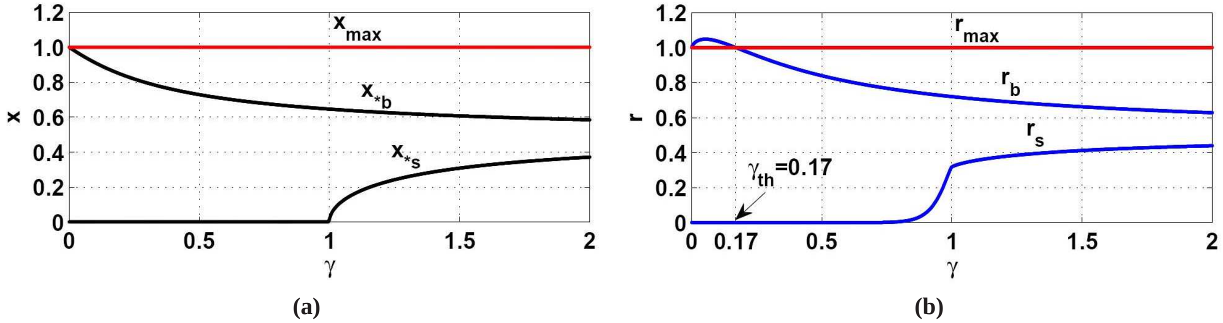


Fig. 5: Coordinates of the bifurcation points (r_b, x_{*b}) and the start points (r_s, x_{*s}) for the first special case case (a) x values and (b) r values..

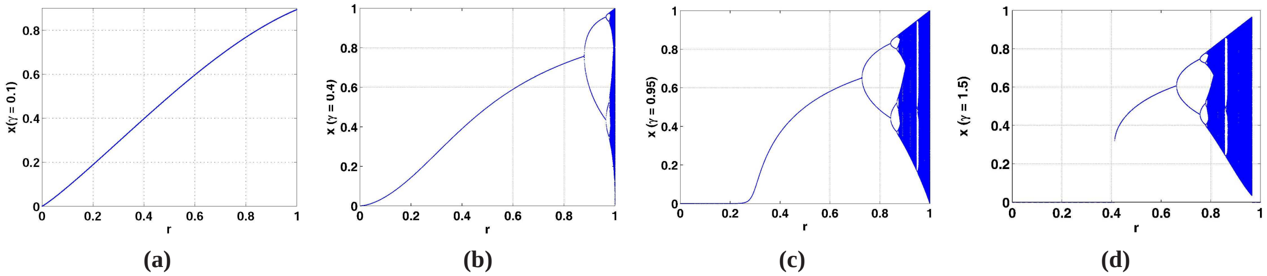


Fig. 6: Bifurcation diagram of the first special case versus r (a) $\gamma = 0.1$, (b) $\gamma = 0.4$, (c) $\gamma = 0.95$ and (d) $\gamma = 1.5$.

changing γ. For example, at $r = 0.9$, the system response changes from fixed point, period two, to chaos when γ equals $0.1, 0.4$, and 0.95, respectively, as shown in Figs. 6(a-c).

Since this special case has another parameter γ, it is possible to study the bifurcation diagram with respect to γ for fixed values of r as shown in Figs. 7(a-c). For $r = 0.3$, only one stable fixed point occurs for all values of $\gamma < 1$. In addition, no nontrivial fixed points exist for $\gamma > 1$. Hence, Fig. 7(a) is consistent with the results given in Fig. 4. For r equals 0.7 and 0.9, the first flip bifurcation occurs at the x and γ values shown in Fig. 7(b) and Fig. 7(c). These values are also consistent with the values given in Fig. 5.

2.3 Maximum Lyapunov Exponent

To prove the chaotic behavior of the output response, it is necessary to have a positive value of the Lyapunov exponent. There are many numerical techniques to calculate the value of Lyapunov exponent. For the 1D map defined by $x_{k+1} = f(x_k, r)$, the maximum Lyapunov exponent (MLE) for the orbit starting at x_0 can be calculated by

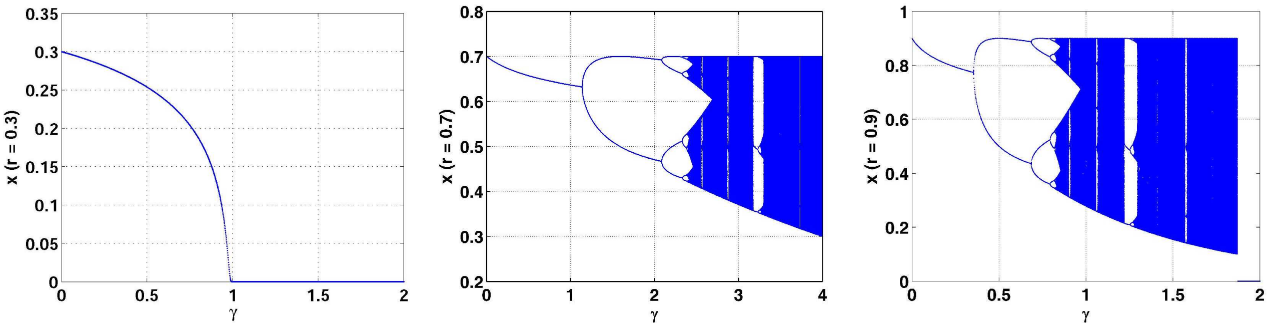
$$MLE = \lim_{n\to\infty}\left(\frac{1}{n}\sum_{i=0}^{n-1}\ln|f'(x_i)|\right). \tag{7}$$

where $f'(x)$ is the derivative of the function $f(x)$.

The MLE of the proposed map is shown in Fig. 8(a) for different values of γ when $r = 0.7$. Comparing this figure with the corresponding bifurcation diagram of Fig. 7(b) demonstrates how MLE characterizes chaos. For instance, when $r = 0.7$ and $\gamma = 0.5$, there is one fixed point in Fig. 7(b) and the MLE in Fig. 8(a) is negative. When $r = 0.7$ and $\gamma = 2.0$, there are two fixed points and MLE is still negative. As γ increases from 2.5 to 4.0 chaos exists and MLE becomes positive and increases, which indicates that chaos becomes more pronounced as γ increases.

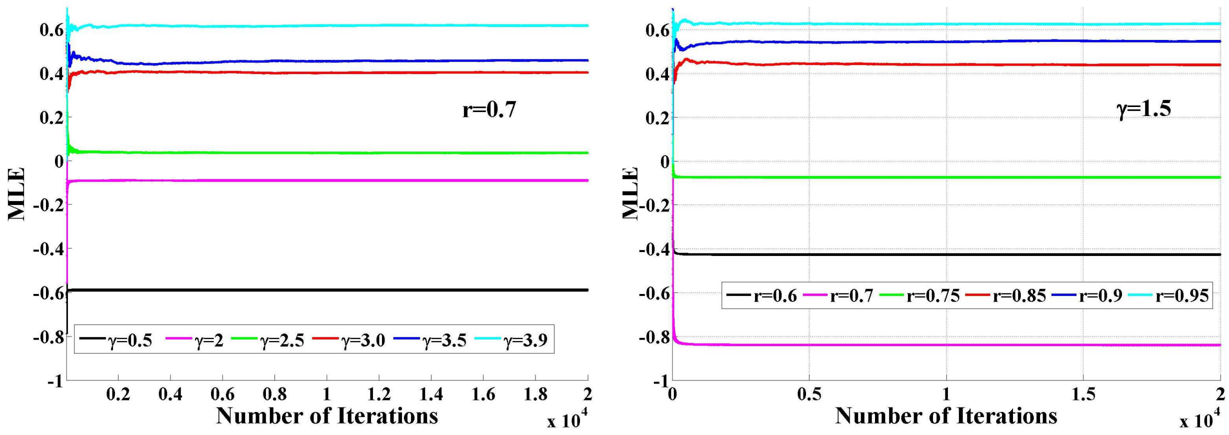
On the other hand, Fig. 8(b) plots MLE for different values of r when $\gamma = 1.5$. Comparing this figure with the corresponding bifurcation diagram in Fig. 6(d), it is clear that there is no chaos for r below 0.8 as MLE is negative and the bifurcation diagram shows fixed points.

In general, Fig. 9 shows 3D and contour plots of the MLE against a sub-region in the r-γ plane. The right edge in the contour plot is consistent with the bifurcation diagrams of $\gamma > 1$ in Fig. 6(d) where the chaotic region can terminate before r reaches unity. Figure10(a) shows the cobweb diagram of the first special case when $r = 0.9$ and $\gamma = 1.8$ and Fig. 10(b) shows the corresponding time series. Those two diagrams further confirm the chaotic behavior, which is indicated by the positive MLE given in Fig. 9.



(a) (b) (c)

Fig. 7: Bifurcation diagrams of the first special case versus γ (a) $r = 0.3$, (b) $r = 0.7$ and (c) $r = 0.9$.



(a) (b)

Fig. 8: MLE of the first special case (a) $r = 0.7$ (b) $\gamma = 1.5$.

3 Chaotic Behavior When $\beta \neq 1$ and $\alpha = \gamma = 1$

Assuming that $f(x,r,\beta) = r\sin(\pi x^{\beta})$, then the peak of this function equals r and it exists at $x = x_p = (0.5)^{1/\beta}$. To ensure that the m^{th} iteration of the function f, $f^{m}(x,r,\beta)$, is enclosed in the interval $[0,1]$, the range of the parameters r and x in this generalized Sine map is set to $r, x \in [0,1]$ in all cases independent of β.

3.1 Nontrivial Fixed Points

The fixed-points analysis for the second special case is similar to the corresponding analysis for the first special case. For $\beta < 1$, only one nontrivial fixed point can exist. For $\beta > 1$, there can be zero, one, or two nontrivial fixed points depending on the values of r and β. The fixed points can be numerically calculated for different values of the parameters r and β by solving $x_{*} = f(x_{*}, r, \beta)$

The critical bifurcation point (r_b, x_{*b}) can only occur when $f'(x_{*b}, r_b, \beta) = -1$ (i.e., flip bifurcation). Hence, r_b, x_{*b} and the equation of the bifurcation curve are given by the following equations, respectively:

$$r_b = \frac{x_{*b}}{\sin(\pi x_{*b}^{\beta})}, \tag{8}$$

$$\pi\beta x_{*b}^{\beta} + \tan(\pi x_{*b}^{\beta}) = 0, \tag{9}$$

$$sin^{-1}\left(\frac{x_{*b}}{r_b}\right)\ln\left(\frac{sin^{-1}\left(\frac{x_{*b}}{r_b}\right)}{\pi}\right) + \frac{x_{*b}\ln(x_{*b})}{\sqrt{r_b^2 - x_{*b}^2}} = 0. \tag{10}$$

Equation (9) is similar to (4) except for the power of x_{*b}. Hence, the following relation can be concluded:

$$(x_{*b}|_{Second\,special\,case})^{\beta} = x_{*b}|_{First\,special\,case} \tag{11}$$

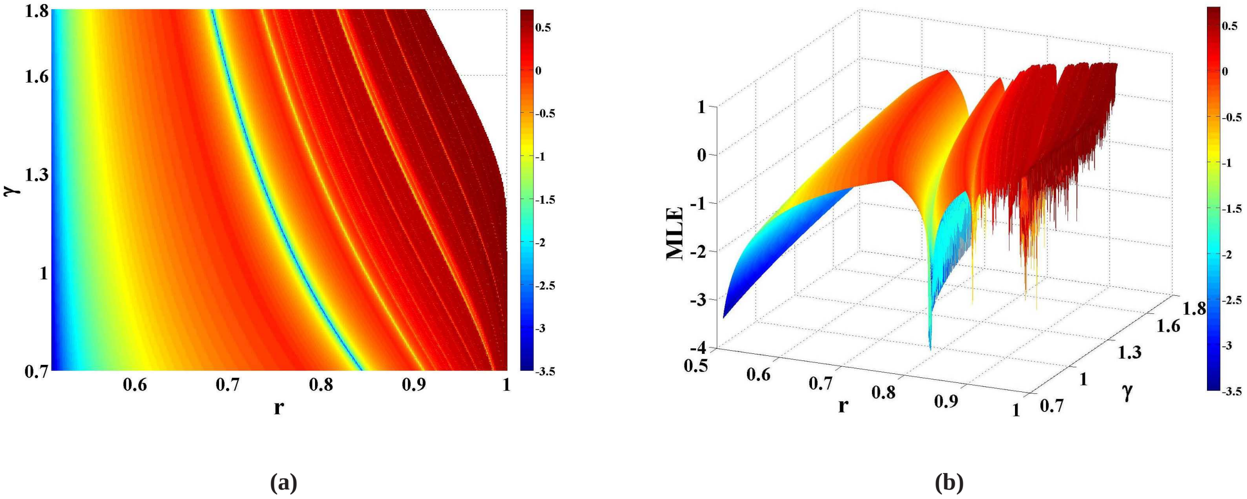


Fig. 9: MLE in the r-γ plane (a) 3D plot (b) contour plot.

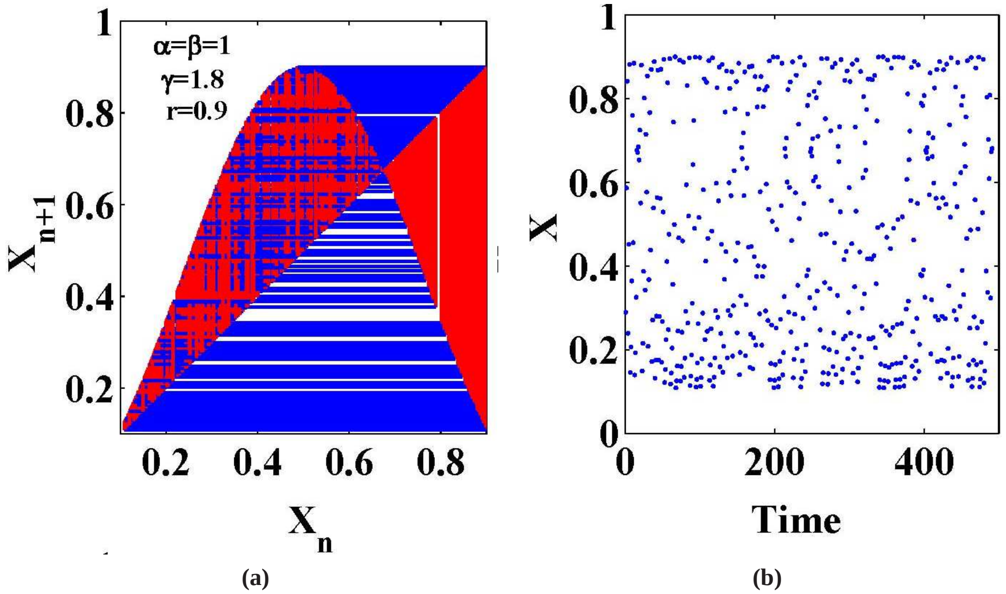


Fig. 10: (a) Cobweb diagram and (b) time series of the first special case.

For $\beta > 1$, the fold bifurcation point (r_s, x_{*s}) at which the nontrivial fixed-points start to appear is obtained by solving $f'(x_*, r, \beta) = 1$ and the following relation can be obtained:

$$(x_{*s}|_{Second\ special\ case})^{\beta} = x_{*s}|_{First\ special\ case} \qquad (12)$$

The following flip bifurcation point (r_b, x_{*b}) occurs when $f'(x_*, r, \beta) = -1$ similar to the case when $\beta \leq 1$.

Figure 11 depicts the values of r_b and x_{*b} against β. Because the parameter r in this map is also restricted to $r \in [0,1]$, then there is no bifurcation at all when $\beta < \beta_{th} = 0.17$. Figure 11 also shows the values of the fold bifurcation points (r_s, x_{*s}) at which the nontrivial fixed-points start to occur when $f'(x_{*s}, r_s, \beta) = 1$. As $\beta_{th} \leq \beta \leq 1$, the value of $x_{*s} = 0$ which means that the nontrivial fixed points start from $x = 0$ as shown in Fig. 12(a). However, the value of r_s begins to increase as β

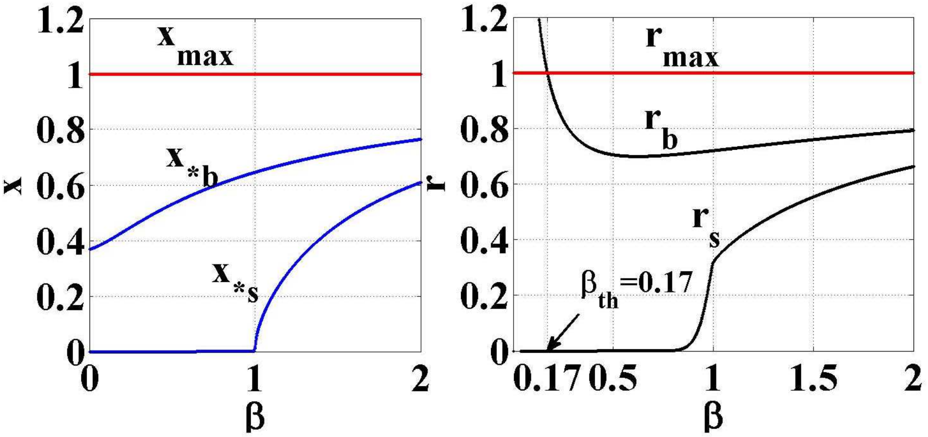


Fig. 11: Coordinates of the bifurcation points (r_b, x_{*b}) and the start points (r_s, x_{*s}) for the second special case.

increases. In Fig. 12(a), $\beta = 0.95$ and the nontrivial fixed points start at the corresponding r_s given in Fig.11. When $\beta > 1$, there is a discontinuity in the bifurcation diagram as the nontrivial fixed points start to appear for nonzero values of both r_s and x_{*s} as shown in Figs. 12(b, c).

3.2 *Bifurcation Diagrams and MLE*

Although the bifurcation diagrams are different from those of the first special case, the general discussions of Sections 2.2 apply. Figure 12 illustrates the differences and progress of the diagram versusu $r \in [0,1]$ as β increases. It shows that as β exceeds 1, two supplementary fixed points are caused by the fold bifurcation at (r_s, x_{*s}) given in Fig. 11(b). Then, a flip bifurcation occurs at (r_b, x_{*b}) given in Fig. 11.

On the other hand, Fig. 13 shows the bifurcation diagram with respect to β for fixed values of r. For $r = 0.3$, only one stable fixed point occurs for all values of $\beta < 1$. In addition, no nontrivial fixed points exist for $\beta > 1$. Hence, Fig. 13(a) is consistent with the results given in Fig. 11. At $r = 0.86$ and $r = 0.96$, Figs. 13(b, c) show the flip (period-doubling) bifurcations to chaos.

To characterize the chaotic behavior of the output response, the Lyapunov exponent is calculated using Eq. (7). Figure 14 plots the MLE against a sub-region in the r-β plane. Similar to the first special case, the calculated values of the MLE are consistent with the bifurcation diagrams of Figs. 12 and 13. It should be noted that according to (7), the MLE can only be calculated and plotted if $f'(x_i) \neq 0$. This fact, along with the nonzero values of r_s shown in Figs. 11 and 12, explain the occurrence of the left edge in the contour plot of Fig. 14(b).

4 Chaotic Behavior When $\alpha \neq 1$ and $\beta = \gamma = 1$

Assuming that $f(x,r,\alpha) = r\sin(\alpha\pi x)$, then the peak of this function equals r and it exists at $x = x_p = 0.5/\alpha$. To keep the successive positive values for x, then $0 \leq \alpha x \leq 1$ and $0 \leq x \leq 1/\alpha$. Consequently, r should also be limited to $0 \leq r \leq 1/\alpha$. The nontrivial fixed-points start to occur at the point (r_s, x_{*s}) where $x_{*s} = 0$ and $r_s = 1/(\pi\alpha)$ as shown from the fixed point curves in Fig. 15(a). The flip bifurcation point (r_b, x_{*b}) occurs when $f'(x_{*b}, r_b, \alpha) = -1$, which consequently demonstrates that the third special case is a scaling of the conventional Sine map where:

$$\alpha \times (x_{*b}|_{Third\ special\ case}) = x_{*b}|_{Conventional\ map} \qquad (13)$$

Figure 15(b) depicts the values of r_s, r_b, x_{*s}, x_{*b} and r_{max} against α for $0.4 \leq \alpha \leq 2.0$. For a specific value of α, the chaotic region extends between the lower r_b curve and the upper r_{max} curve. Hence, wider chaotic regions are obtained when $\alpha < 1.0$, as depicted in the bifurcation diagrams of Fig. 16(a). Once more, the scaling property is clearly demonstrated in these bifurcation diagrams. Figure 16(b) depicts the contour plot of the MLE against a sub-region in the r-α plane. Comparing this figure with the bifurcation diagrams of Fig. 16(a) further demonstrates how MLE characterizes chaos. The upper edge in the contour plot of Fig. 16(b) is due to the fact that $r_{max} = \frac{1}{\alpha}$ as shown in Fig. 15(b).

5 Encryption Based on the Generalized Sine Maps

It is clear from the previous sections that the output of the generalized Sine map can be controlled via the four parameters $(r, \alpha, \beta, \gamma)$. The generated MLE diagrams of

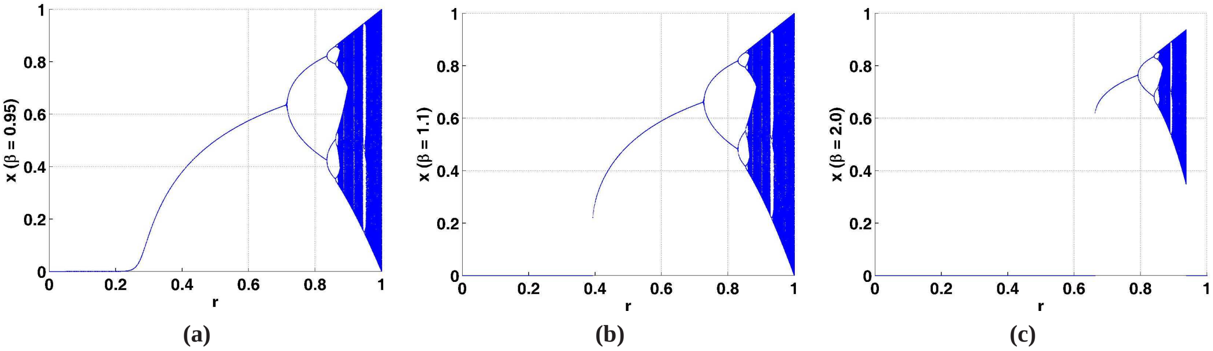


Fig. 12: Bifurcation diagrams of the second special case versus r for (a) $\beta = 0.95$, (b) $\beta = 1.1$, and (c) $\beta = 2.0$.

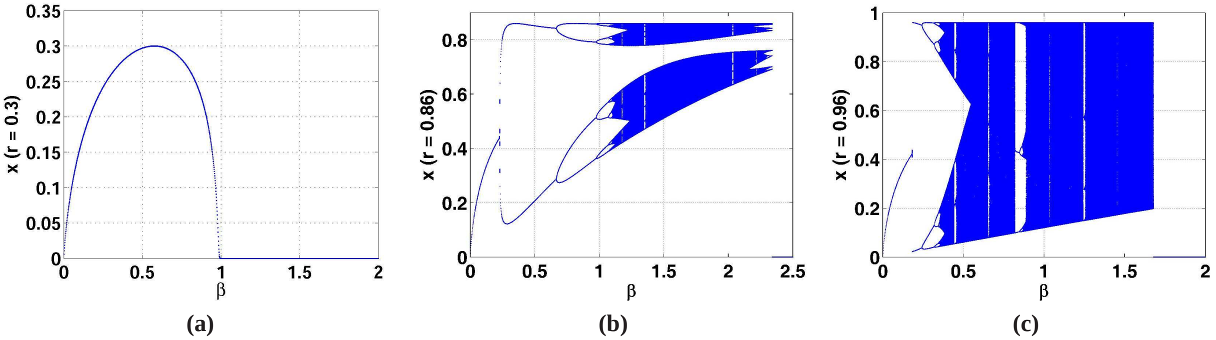


Fig. 13: Bifurcation diagrams of the second special case versus β for (a) $r = 0.3$, (b) $r = 0.86$ and (c) $r = 0.96$.

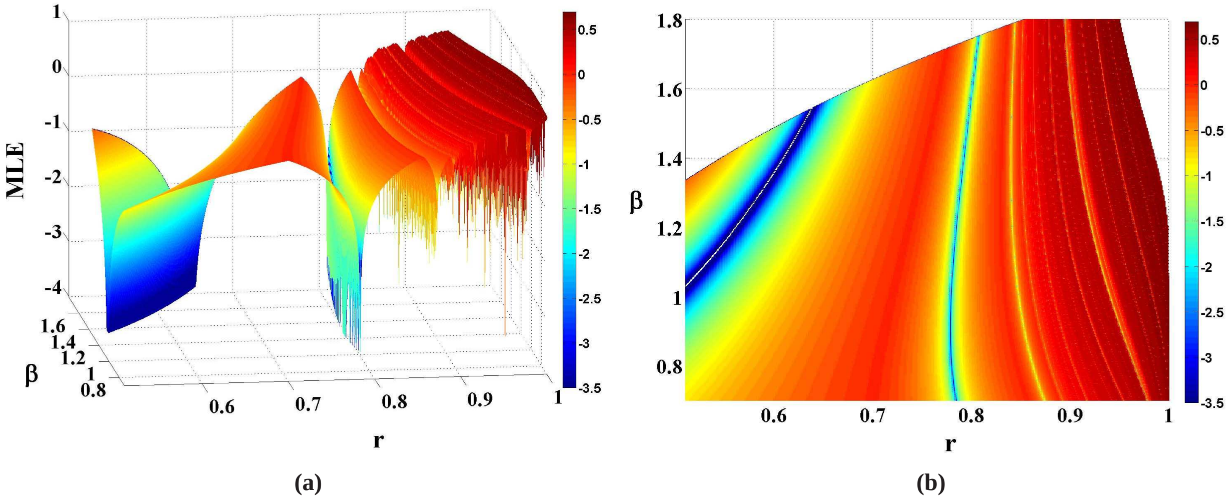
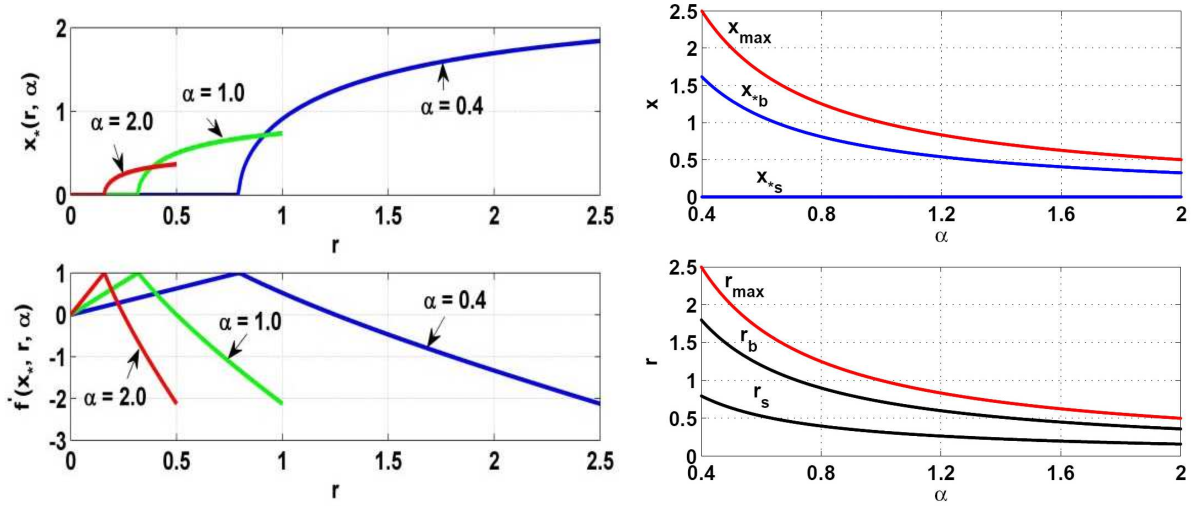


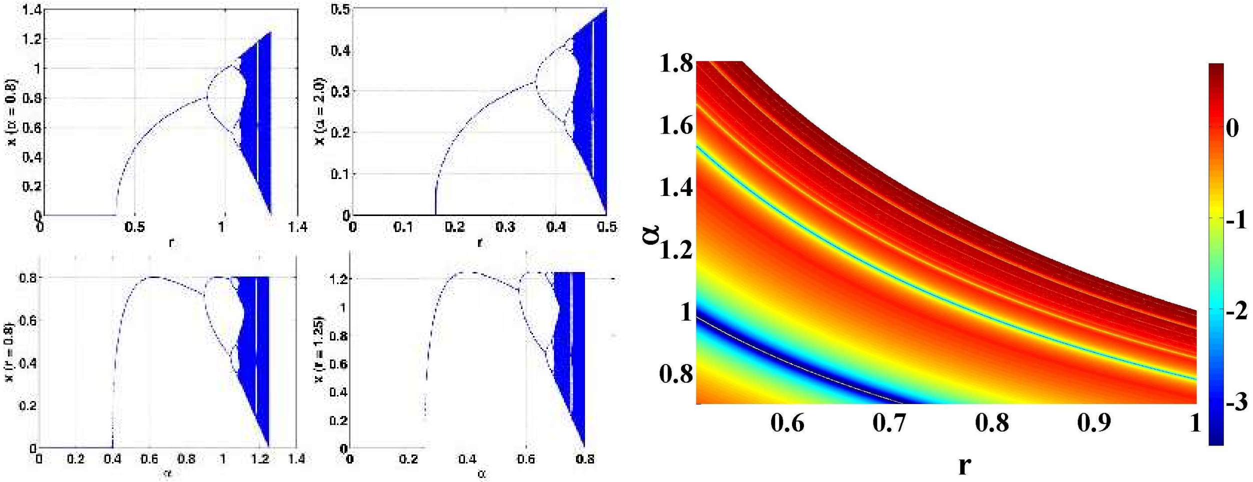
Fig. 14: MLE in the r-β plane (a) 3D plot (b) contour plot.

Figs. 9, 14 and 16 can be used to find common regions of the parameters at which the response behaves chaotically. Figure 17(a) shows the MLE of the generalized Sine map when $r = 0.99$, $\alpha = 1.0$ and for different values of $\beta, \gamma \in [0.5, 1.5]$. While the maximum MLE value in the above range exists at $\beta = 1.048$ and $\gamma = 1.172$ and equals



(a) (b)

Fig. 15: (a) Fixed points and derivatives of $f(x,r,\alpha) = r\sin(\alpha\pi x)$ for different values of α and (b) coordinates of the bifurcation points (r_b, x_{*b}) and the start points (r_s, x_{*s}) for $0.4 \leq \alpha \leq 2.0$.



(a) (b)

Fig. 16: (a) Bifurcation diagram of the third special case for $\alpha = 0.8, 2.0$, and $r = 0.8, 1.25$, and (b) contour plot of the MLE for the third special case.

MLE$_{max}$ $\approx$ 0.65, the MLE in the conventional case $(\beta = 1, \gamma = 1)$ is 0.603.

Sensitivity analysis of the Sine map parameters is studied in Fig. 17(b), which shows the cross correlation of the parameters r, β and γ through simulating the map twice and introducing an error in the second run in one parameter only while fixing other values. The point at which the correlation coefficient becomes maximum (≈ 1) indicates that the map is insensitive to the error introduced in the second run.

In order to demonstrate the benefits of using the generalized forms of the Sine map, Fig. 18 depicts the block diagram of a simple encryption that utilizes it and its equivalent decryption block diagram. To focus on the effect of utilizing the generalized map, this initial encryption system only involves pixel-value substitutions that are described as follows.

–**Substitutions:** At the beginning, the parameters and initial values of the generalized Sine maps are calculated from the system key. For each pixel in the input image, a new output value is generated from the three Sine maps. The encrypted pixel is produced by XORing the three color channels of the input pixel with the three outputs from the Sine maps and the three color channels of the previously encrypted pixel. This encrypted pixel is then delayed and multiplexed for utilization in the next pixel encryption cycle. As shown in Fig. 18(b), the decryption system is the reverse of the encryption system.

Table 1 shows the multiplexing table used in the system block diagram. Based on the Least Significant Bit (LSB) of the Red (R), Green (G) and Blue (B) channels, the multiplexer output is determined. While the multiplexing block works as a nonlinear element that improves the differential attack measures, the delay block improves the pixel correlation coefficients. It should be noted that the initial delay for the first pixel is chosen as zero.The decimal values generated from the maps, $X_i, i = 1,2,3$, are transformed into integer values in the range from 0 to 255 using the following equation:

$$Xnew_i = INT\,(X_i \times sf_1)\,MOD\,256. \quad (14)$$

where the INT function returns the integer part of a number, the MOD function returns the remainder of integer division and the scaling factor sf_1 is selected so that the resulting 8 bits of $Xnew_i$ are highly chaotic. Hence, $Xnew_1, Xnew_2$ and $Xnew_3$ are XORed with the R, G and B channels of the input pixel, respectively.

To accomplish Shannon's confusion and diffusion properties, a good image encryption scheme should consist of two main permutations and substitutions phases [16]. While the permutations phase changes the pixels' positions, the substitutions phase changes the pixels' values, usually using a pseudo random number generator. The initially described encryption system of Fig. 18 involves substitutions only to demonstrate the good effect of utilizing the generalized Sine map. To improve the security of the encryption system, a permutations phase is added as shown in Fig. 19. This figure shows a permutations-substitutions encryption system as well as its corresponding decryptions system. Compared to Fig. 18, only the permutations phase is added, which is described as follows.

–**Permutations:** The Arnold's cat map, which is a very well-known technique for pixel permutations, is used [31]. The generalized 2D Arnold's cat map is defined as:

$$\begin{pmatrix} x_{new} \\ y_{new} \end{pmatrix} = \begin{pmatrix} 1 & a \\ b & 1+ab \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} MOD\,M, \quad (15)$$

where $a,b \in \{1,2,\ldots,M-1\}$, M is the square image size, $x,y \in \{1,2,\ldots,M\}$ represent the pixel column and row positions in the image respectively and x_{new}, y_{new} give the new column and row positions for the pixel under transformation, respectively. The permutations phase is designed to be dependent on the input plain image by calculating the algebraic sum of the input image three color channels as follows.

Table 1: Multiplexing Table

Selection Bits			Output		
R_{LSB}	G_{LSB}	B_{LSB}	R_{out}	G_{out}	B_{out}
0	0	0	B	R	G
0	0	1	G	B	R
0	1	0	R	G	B
0	1	1	B	R	G
1	0	0	G	B	R
1	0	1	R	B	G
1	1	0	B	G	R
1	1	1	G	R	B

$$P_{Sum} = R_{Sum} + G_{Sum} + B_{Sum}, \quad (16)$$

where R_{Sum}, G_{Sum} and B_{Sum} are the sums of the red, green and blue channels of the input image, respectively. Then, the Arnold's cat map parameters a and b are calculated using the system key and P_{Sum}.

The next subsection will explain the design of the system key and how to compute the permutation and substitution parameters from it.

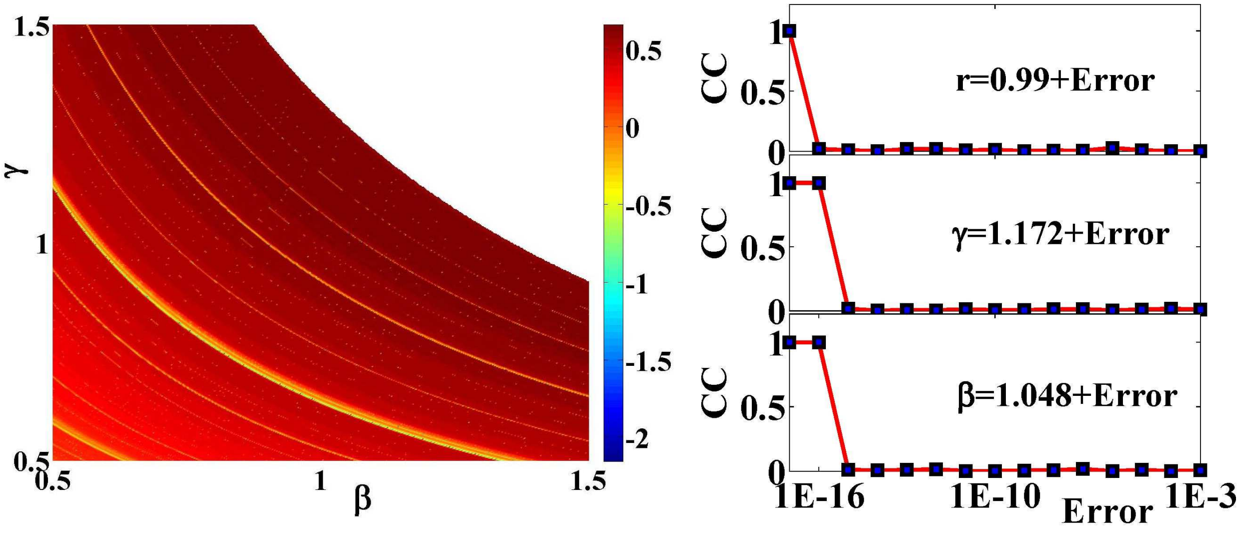
5.1 System Key

Based on the block diagrams of Fig. 19, the system key consists of two parts; one part is for the substitution parameters and the other part is for the permutation parameters. The permutation parameters include L bits to store the $M \times M$ size of the image being encrypted. If $L = ceil(log_2 M)$, then L needs 4 bits to define the image size. In addition, two L-bit integers a_{key} and b_{key} are used for the Arnold's cat map parameters. Hence, the length of this part is $(4 + 2 \times ceil(log_2 M))$.The parameter values obtained from the system key, a_{key} and b_{key}, are modified according to (17) and (18) to get the Arnold cat map parameters a and b.

$$a = MOD\,(P_{Sum} + a_{key}, M-1) + 1, \quad (17)$$

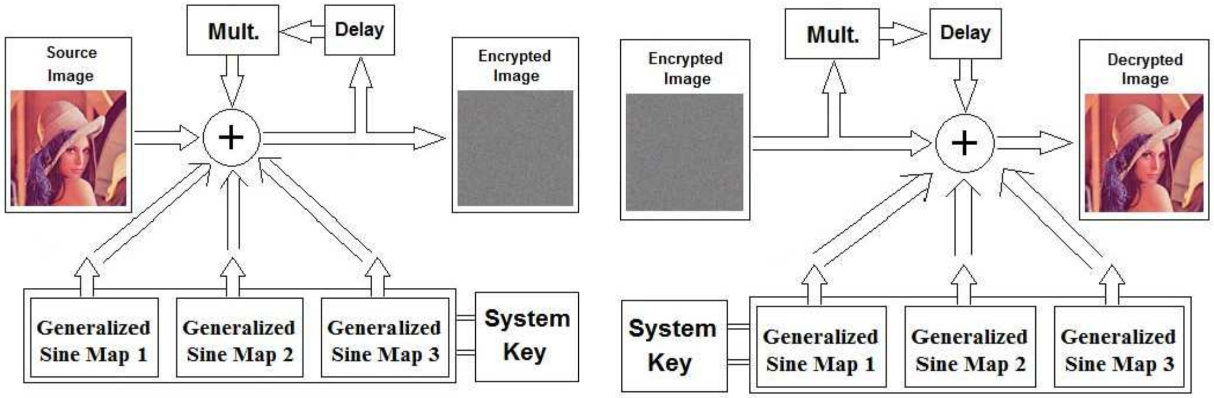
$$b = MOD\,(P_{Sum} + b_{key}, M-1) + 1. \quad (18)$$

The substitutions part can consist of 15 variables (4 parameters for each generalized Sine map and 3 initial values). Assuming that the register size is 32 bits, then this part can reach up to 480 bits. However, in order to design a key with an appropriate length and good sensitivity, Fig. 20 shows the proposed key structure. The substitutions part of the key consists of four 32 bit values $V1$ to $V4$. Hence, 128 bits are used to fill-up the required 480 bits with a random distribution that makes every bit of the key affect many parameters. Hence, the total length of the key is $(4 + 2 \times ceil\,(log_2 M) + 128)$ bits, where M



(a) (b)

Fig. 17: (a) The MLE versus the β-γ plane, and (b) sensitivity of the parameters r, γ and β.



(a) (b)

Fig. 18: Encryption based on substitutions only: (a) encryption block diagram and (b) decryption block diagram.

is the square image size. For an image of size 1024×1024, $M = 1024$, $L = ceil\,(log_2 M) = 10$ and the total key length is 152 bits.

Each of the values Vi is divided into four sub-values Vi_j of 8 bits each $i, j \in \{1,2,3,4\}$. These 16 sub-values are utilized in constructing the 15 parameters and initial values of the generalized Sine maps. An example of this construction is given in Fig. 20. In any such construction, each sub-value Vi_j should affect different parameters or initial conditions of the three maps. Consequently, each value Vi affects all parameters and initial conditions of the three maps. The main idea behind this construction is that any single bit change in the system key affects more than one parameter or initial condition of the three maps and, hence, improves key sensitivity.

In order to keep the Sine maps in the chaotic range, each parameter S and initial value Xo are calculated from the key, shown in Fig. 20, as follows:

$$S = S_f + K\_S \times sf_2 \qquad (19)$$

$$Xo = K\_Xo \times sf_3 \qquad (20)$$

where S_f is the fixed part of the parameter and K_S is the integer value obtained from the key. The scaling factor sf_2 ensures that the first two decimal places of S_f are not affected. Those fixed parts and scaling factors of the

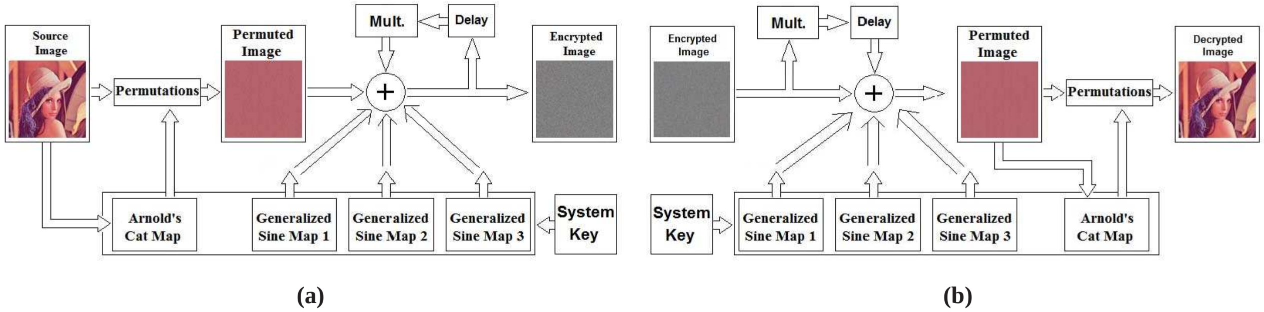
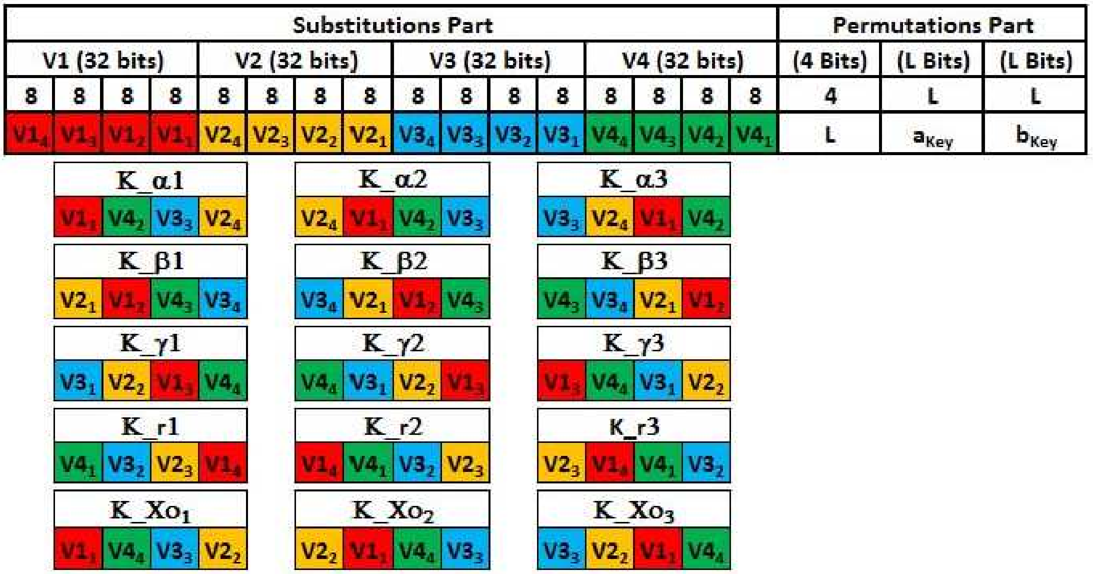


Fig. 19: Encryption based on permutations and substitutions: (a) encryption block diagram and (b) decryption block diagram.



Substitutions Part																Permutations Part		
V1 (32 bits)				V2 (32 bits)				V3 (32 bits)				V4 (32 bits)				(4 Bits)	(L Bits)	(L Bits)
8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	4	L	L
$V1_4$	$V1_3$	$V1_2$	$V1_1$	$V2_4$	$V2_3$	$V2_2$	$V2_1$	$V3_4$	$V3_3$	$V3_2$	$V3_1$	$V4_4$	$V4_3$	$V4_2$	$V4_1$	L	a_{Key}	b_{Key}

K_α1				K_α2				K_α3			
$V1_1$	$V4_2$	$V3_3$	$V2_4$	$V2_4$	$V1_1$	$V4_2$	$V3_3$	$V3_3$	$V2_4$	$V1_1$	$V4_2$
K_β1				**K_β2**				**K_β3**			
$V2_1$	$V1_2$	$V4_3$	$V3_4$	$V3_4$	$V2_1$	$V1_2$	$V4_3$	$V4_3$	$V3_4$	$V2_1$	$V1_2$
K_γ1				**K_γ2**				**K_γ3**			
$V3_1$	$V2_2$	$V1_3$	$V4_4$	$V4_4$	$V3_1$	$V2_2$	$V1_3$	$V1_3$	$V4_4$	$V3_1$	$V2_2$
K_r1				**K_r2**				**K_r3**			
$V4_1$	$V3_2$	$V2_3$	$V1_4$	$V1_4$	$V4_1$	$V3_2$	$V2_3$	$V2_3$	$V1_4$	$V4_1$	$V3_2$
K_Xo$_1$				**K_Xo$_2$**				**K_Xo$_3$**			
$V1_1$	$V4_4$	$V3_3$	$V2_2$	$V2_2$	$V1_1$	$V4_4$	$V3_3$	$V3_3$	$V2_2$	$V1_1$	$V4_4$

Fig. 20: Example utilization of the system key in constructing the parameters and initial conditions of the three maps.

parameters are chosen to guarantee that the generalized Sine map will maintain its chaotic behavior for any choice of the system key. Similarly, K_Xo is the integer value obtained from the key and the scaling factor sf_3 ensures that the initial values are in the interval $(0,1)$.

5.2 Encryption Results

In this subsection, standard evaluation criteria are used to test the performance of the encryption systems [32, 33, 34]. These criteria include pixel correlation coefficients, histogram distributions and NIST statistical test suite. The sensitivity of the encryption system to small changes in the input is evaluated using differential attack measures. Those measures include the Mean Absolute Error (MAE), Number of Pixels Change Rate (NPCR) and Unified Average Changing Intensity (UACI) [33]. The sensitivity of the system key to only one bit change is discussed using the Mean Square Error (MSE) and entropy.

The used values of the scaling factors sf_1, sf_2 and sf_3 are $10^{12}, 10^{-12}$ and 10^{-10}, respectively. The used fixed values of the generalized Sine maps' parameters are $\{\alpha_f, \beta_f, \gamma_f, r_f\} = \{1, 1.172, 1.048, 0.99\}$. As previously mentioned and demonstrated by Fig. 17, those fixed values and scaling factors ensure operation in the chaotic region of the generalized Sine map for any given system key. The key for the permutations-substitutions system is chosen as: $''F1219959A7E9F7D773B2B6C9D6F66900A0641E''_{(hex)}$. The same key, without the last six hexadecimal digits, is used for the substitutions system. Using those keys, the

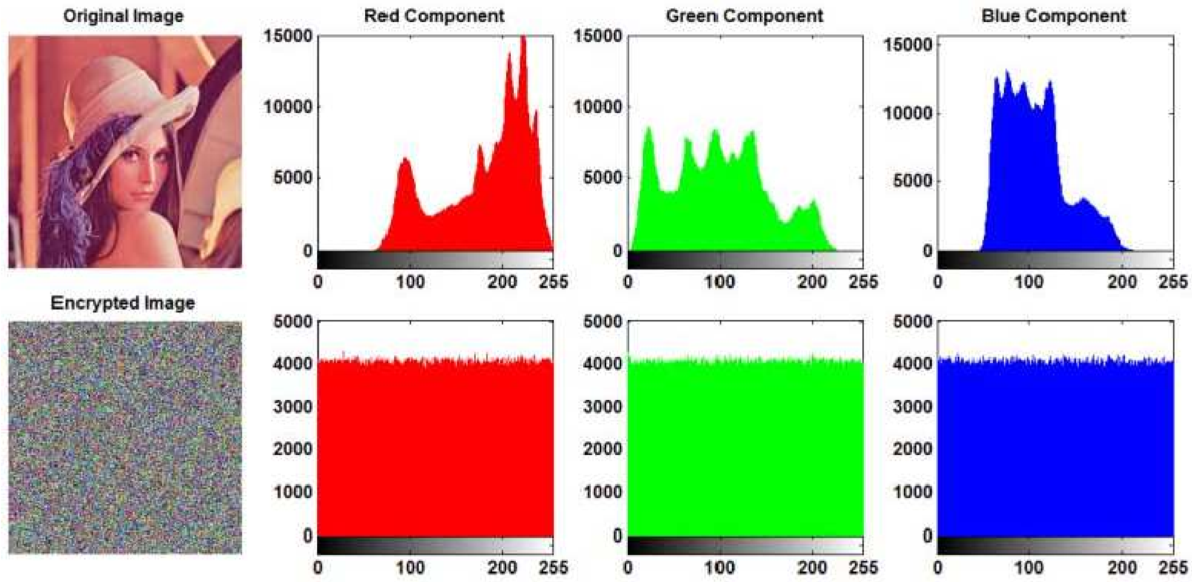


Fig. 21: Histogram distributions for the original Lena image (first row) and its encrypted image based on substitutions only (second row).

Table 2: Analysis Results of the Proposed Encryption Systems

Color	Substitutions Only			Permutations-Substitutions					
	Pixel Correlations			Pixel Correlations			Differential Attack Measures		
	Horz.	Vert.	Diag.	Horz.	Vert.	Diag.	MAE	NPCR(%)	UACI(%)
R	0.0006	0.0011	0.0011	0.0002	0.0005	-0.0004	84.1717	99.6092	33.4540
G	0.0007	0.0001	0.0008	-0.0001	-0.0004	-0.0011	78.0309	99.6109	33.4498
B	0.0003	0.0005	0.0010	-0.0003	0.0008	-0.0003	70.3813	99.6089	33.4998
Avg.	0.0005	0.0006	0.0010	0.0002	0.0005	0.0006	77.5280	99.6096	33.4679

Table 3: NIST Suite Results of the Proposed Encryption Systems for Lena (1024×1024)

Test	Subst.		Perm.-Subst.	
	PV	PP	PV	PP
Frequency	✓	1.000	✓	1.000
Block Frequency	✓	0.958	✓	1.000
Cumulative Sums	✓	1.000	✓	0.979
Runs	✓	0.958	✓	1.000
Longest Run	✓	1.000	✓	1.000
Rank	✓	1.000	✓	1.000
FFT	✓	1.000	✓	0.958
Non Overlapping Template	✓	0.991	✓	0.992
Overlapping Template	✓	1.000	✓	1.000
Universal	✓	0.958	✓	0.958
Approximate Entropy	✓	1.000	✓	1.000
Random Excursions	✓	1.000	✓	0.967
Random Excursions Variant	✓	0.997	✓	0.993
Serial	✓	0.979	✓	1.000
Linear Complexity	✓	0.958	✓	0.958
Final Result	**Success**		**Success**	

calculated parameters and initial condition of the three generalized maps are $\{\alpha,\beta,\gamma,r,x_0\} = \{1.0015001, 1.1756172, 1.0513884, 0.9900120, 0.1507243\}$, $\{1.0028077, 1.1739435, 1.0516036, 0.9940434, 0.4149860\}$ and $\{1.0029973, 1.1761348, 1.0485677, 0.9939249, 0.3002555\}$, respectively. In addition, the parameters of the Arnold's cat map are $\{a_{key}, b_{key}\} = \{25, 30\}$.

The systems are tested using the color Lena image (1024×1024). Figure 21 shows the histograms of the original and encrypted Lena image using substitutions only. The uniform distributions of the encrypted image represent a positive sign for the quality of the substitutions using the generalized map. Table 2 shows the pixel correlation coefficients due to the substitutions system as well as due to the permutations-substitutions system. The analysis results are promising as they give low correlation coefficients due to the substitutions system and even lower values for the permutations-substitutions system. The differential attack measures for the permutations-substitutions system are also given in Table 2. These measures analyze the

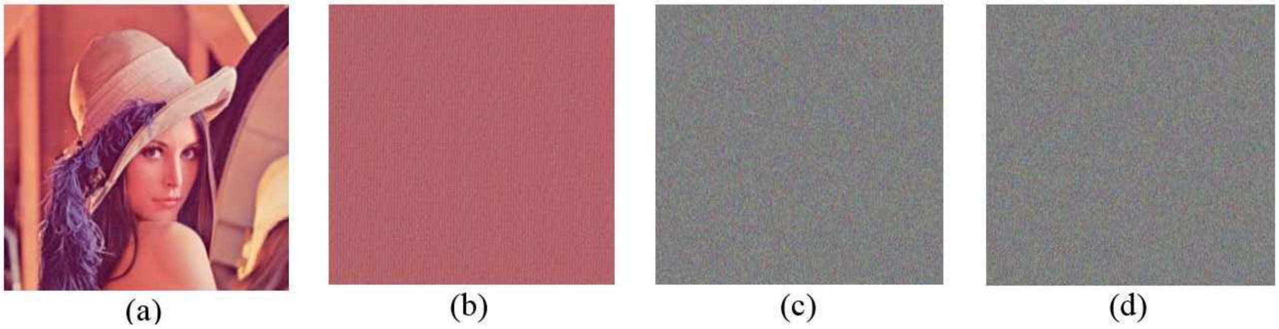


Fig. 22: (a) Lena image, (b) permuted image, (c) encrypted image using permutations and substitutions and (d) encrypted image using permutations and substitutions after changing one pixel in the plain image.

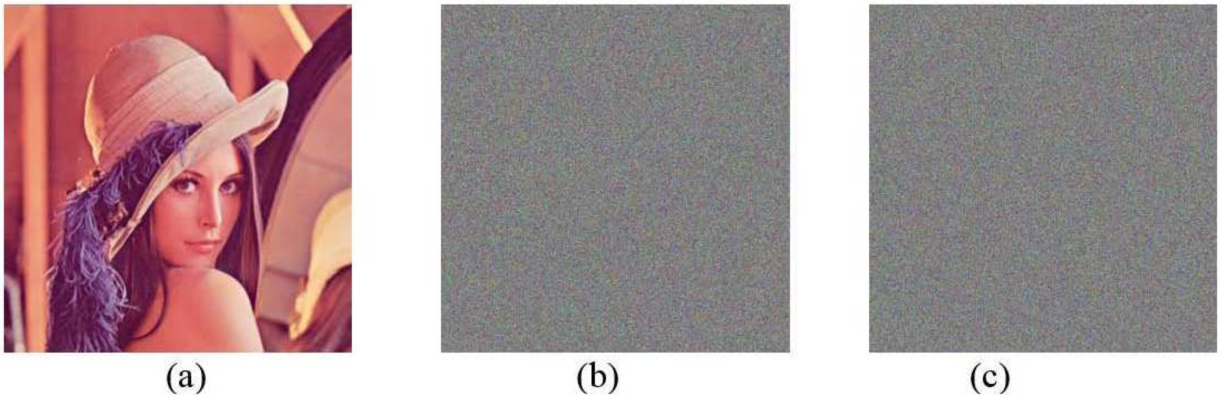


Fig. 23: Decrypted Lena image with one bit change in the key for (a) Case I, (b) Case II and (c) Case IV.

Table 4: MSE and Entropy as Measures of Sensitivity

Case		MSE			Entropy	
	Red	Green	Blue	Red	Green	Blue
I	0.00	0.00	0.00	7.2516	7.5919	6.9491
II	10628.82	9038.22	7074.75	7.9998	7.9998	7.9998
III	10636.14	9072.22	7086.55	7.9998	7.9998	7.9998
IV	10626.49	9068.54	7094.82	7.9998	7.9998	7.9998
V	10642.08	9055.04	7099.60	7.9998	7.9998	7.9998

sensitivity of the encryption system to one-pixel change in the input plain image and they are in the expected good ranges [33]. In Table 3, the NIST statistical test suite results are provided. The success in all of the 15 tests indicates that the output is almost random and that the encryption systems are effective despite their simplicity.

It should be noted that when calculating the differential attack measures, two plain images with only one pixel difference produce different ciphered images. For instance, changing one pixel at the last location, i.e., location $(1024,1024)$, in the Lena image and encrypting both the original and the modified plain images using the permutations-substitutions system produces the ciphered images given in Figs. 22(c) and 22(d), respectively. The cross correlation and MSE values between the red, green and blue channels of the images in Figs. 22(c) and 22(d) are $(-0.0004, 0.0014, -0.0006)$ and (10918.50, 10915.65, 10925.23), respectively. Even if we consider an all-zero color plain image and an all-zero color plain image except for one nonzero pixel at the end, the ciphered images are different. For example, if we encrypt two such plain images, the two ciphered images become different with cross correlation and MSE values in the red, green and blue channels of $(0.0003, -0.0007,$

Table 5: Results of Encrypting Different Standard Images

Img.	Col.	Original Image Corr.			Encrypted Image Corr.			Entropy		MAE	NPCR	UACI
		Horz.	Vert.	Diag.	Horz.	Vert.	Diag.	Orig.	Enc.		(%)	(%)
Mandrill 4.2.03	R	0.9231	0.8660	0.8543	-0.0012	-0.0009	-0.0011	7.7067	7.9992	76.3814	99.5922	33.5660
	G	0.8655	0.7650	0.7348	-0.0017	0.0025	-0.0018	7.4744	7.9994	72.9883	99.6128	33.4639
	B	0.9073	0.8809	0.8399	-0.0002	0.0001	0.0024	7.7522	7.9993	79.6467	99.6067	33.4833
Peppers 4.2.07	R	0.9606	0.9615	0.9533	-0.0017	0.0015	-0.0001	6.3319	7.9992	72.7905	99.6128	33.4633
	G	0.9828	0.9830	0.9767	0.0029	-0.0034	-0.0044	6.4072	7.9993	85.7679	99.6040	33.4842
	B	0.9582	0.9599	0.9483	0.0029	-0.0017	-0.0015	6.1304	7.9993	87.5711	99.6071	33.4636
Airplane 4.2.05	R	0.9726	0.9568	0.9343	-0.0049	-0.0010	-0.0015	6.7178	7.9994	81.5433	99.6071	33.3853
	G	0.9578	0.9678	0.9326	-0.0010	-0.0008	-0.0002	6.7990	7.9992	84.2761	99.6105	33.4674
	B	0.9640	0.9353	0.9146	0.0026	0.0001	-0.0042	6.2138	7.9994	83.4903	99.6109	33.4496
Bout 4.2.06	R	0.9558	0.9541	0.9420	-0.0015	-0.0003	-0.0001	7.3124	7.9993	71.2405	99.5964	33.4416
	G	0.9715	0.9663	0.9530	-0.0006	-0.0006	-0.0032	7.6429	7.9992	87.5358	99.6334	33.3972
	B	0.9710	0.9694	0.9530	0.0027	-0.0020	-0.0006	7.2136	7.9992	87.6360	99.6075	33.4986
Splash 4.2.01	R	0.9936	0.9951	0.9894	0.0016	0.0014	-0.0006	6.9481	7.9994	87.1703	99.6250	33.4528
	G	0.9812	0.9871	0.9711	0.0015	0.0022	0.0010	6.8845	7.9994	90.8088	99.6189	33.4045
	B	0.9826	0.9789	0.9649	-0.0026	0.0009	-0.0019	6.1265	7.9993	81.3107	99.6037	33.4556
Black Image	R	1.0000	1.0000	1.0000	-0.0011	0.0023	-0.0007	0.0000	7.9993	127.2606	99.6105	33.4730
	G	1.0000	1.0000	1.0000	0.0007	-0.0005	-0.0033	0.0000	7.9993	127.5760	99.6334	33.4391
	B	1.0000	1.0000	1.0000	0.0001	-0.0015	0.0008	0.0000	7.9993	127.4015	99.6155	33.4736

Table 6: Comparison with Other Systems

	Pixel Correlations			NPCR	UACI	Entropy
	Horz.	Vert.	Diag.	(%)	(%)	
This Work	**0.0051**	**0.0029**	**0.0014**	**99.61**	**33.51**	**7.999**
[18]	0.0058	0.0026	0.0024	99.61	33.45	7.991
[19]	0.0095	0.0112	0.0283	99.61	33.40	7.999
[20]	0.0014	0.0020	0.0018	99.61	33.45	7.999

Table 7: Comparison Between the Main Effects of the Newly Introduced Sine Map Parameters

Case	First	Second	Third
	$x_{n+1} = r \sin^{\gamma}(\pi x_n)$	$x_{n+1} = r \sin(\pi x_n^{\beta})$	$x_{n+1} = r \sin(\alpha \pi x_n)$
Range	$r, x_n \in [0,1], \gamma > 0$	$r, x_n \in [0,1], \beta > 0$	$r, x_n \in [0, 1/\alpha], \alpha > 0$
Critical Values	• $x_p = 0.5$ • $\gamma \leq 1 : x_{*s} = 0$ • $\gamma > 1 : \pi \gamma x_{*s} - \tan(\pi x_{*s}) = 0$ • $r_s = \frac{x_{*s}}{\sin^{\gamma}(\pi x_{*s})}$	• $x_p = (0.5)^{(1/\beta)}$ • $\beta \leq 1 : x_{*s} = 0$ • $\beta > 1 : \pi \beta x_{*s}^{\beta} - \tan(\pi x_{*s}^{\beta}) = 0$ • $r_s = \frac{x_{*s}}{\sin(\pi x_{*s}^{\beta})}$	• $x_p = 0.5/\alpha$ • $x_{*s} = 0$ • $r_s = \frac{1}{\pi \alpha}$
Bifurcation	• No bifurcation if $\gamma < \gamma_{th} = 0.17$ • Flip points (r_b, x_{*b}) : $\pi \gamma x_{*b} + \tan(\pi x_{*b}) = 0$ $r_b = \frac{x_{*b}}{\sin^{\gamma}(\pi x_{*b})}$ • $\gamma > 1$: Fold points at (r_s, x_{*s})	• No bifurcation if $\beta < \beta_{th} = 0.17$ • Flip points (r_b, x_{*b}) : $\pi \beta x_{*b}^{\beta} + \tan(\pi x_{*b}^{\beta}) = 0$ $r_b = \frac{x_{*b}}{\sin(\pi x_{*b}^{\beta})}$ • $\beta > 1$: Fold points at (r_s, x_{*s})	• Flip points (r_b, x_{*b}) : $\pi \alpha x_{*b} + \tan(\alpha \pi x_{*b}) = 0$ $r_b = \frac{x_{*b}}{\sin(\alpha \pi x_{*b})}$

-0.0002) and (10929.74, 10922.61, 10918.58), respectively.

5.3 Key Sensitivity Analysis

In order to test the sensitivity of the system to one bit change in the key, the following cases are examined during decryption.

–Case I: Exact Key
–Case II: one bit change in the LSB of V1
–Case III: one bit change in the LSB of V2
–Case IV: one bit change in the LSB of V3
–Case V: one bit change in the LSB of V4

Figure 23 shows the results for cases I, II and IV. It is obvious that the system is very sensitive to only one bit change in the key. The reason for this key sensitivity is the high sensitivity of the generalized Sine map to any change in the parameters and initial condition. In addition, the design of the system key makes any single bit change affect more than one parameter or initial condition of the three maps. Table 4 shows the MSE and entropy values for each of the five cases. For Case I, the MSE values are zeros and this proves that the decryption system succeeds in recovering the original image as is with no errors. In the other four cases, the MSE values are large, which imply that the decrypted image is not related to the input image. Furthermore, the entropy values approach 8, which indicate that the wrongly decrypted images are almost random.

5.4 Additional Results and Comparisons

In order to test the performance of the permutations-substitutions system with other images, different standard images from the USC-SIPI image database [35], in addition to the black image, are encrypted by the system. Table 5 shows the encryption results, which demonstrate that the system is successful in encrypting different images. Furthermore, the proposed system is compared with other related systems using the color Lena image (256×256). Table 6 shows the results of this comparison and it is clear that the correlation coefficients and the differential attack measures are in the same order as the other systems.

Despite that fact that the structures of the proposed encryption systems are simple, their analysis results are comparable with other recent systems having more complicated structures and operations. The good results obtained by our systems are based on the studied chaotic behavior of the introduced generalized Sine map. However, the other systems given in Table 6 have more complicated structures that either involve 3D continuous chaotic generators [18], several rounds of confusion and diffusion [19] or a confusion-diffusion architecture in which ordinary confusion operations are replaced by a bit-level expand-and-shrink strategy [20]. Furthermore, while the proposed encryption system is controlled by 15 different parameters and initial values of the generalized Sine maps and 2 different parameters of the Arnold's cat map, other systems are controlled by fewer variables (e.g., from 5 to 9 in [18,19,20]).

6 Conclusions and Future Work

In this paper, we have presented a new generalization of the conventional Sine map. In addition to the original parameter of the Sine map, r, the new generalization includes three different parameters γ, β, and α. To analyze the chaotic behavior of the generalized map due to each of the newly added parameters, three special cases have been discussed. In each special case, r and one of the newly introduced parameters are varied and the other two are set to unity.

For each case, we have discussed the fixed points and bifurcation diagrams with respect to the two parameters r and $(\gamma, \beta$, or $\alpha)$. The maximum Lyapunov exponent is also calculated for different values of the parameters r, γ, β and α. In addition, this paper has utilized the newly designed map in two image encryption applications which demonstrate the advantage of the added degrees of freedom. Table 7 provides a brief summary and comparison of the characteristics of the three special cases. Designing and analyzing generalizations of other one dimensional maps should also be considered and compared with the presented generalization. In addition, more encryption systems, which utilize other generalized maps, can be studied and compared with the proposed one.

Acknowledgement

This research was supported financially by the Science and Technology Development Fund (STDF), Egypt, Grant No. 4276.

References

[1] D. Gulick, Encounters with Chaos, McGrawHill, New York, 1992.

[2] M. Ausloos, M. Dirickx, The logistic Map and the Route to Chaos from the Beginnings to Modern Applications, Springer, Berlin/Heidelberg, 2006.

[3] T. Kinnunen, H. Pastijn, Proceedings of the International Conference on Optimization Techniques and Applications, 270-283 (1987).

[4] R. Pearl, An Introduction to Medical Statistics, Oxford Medical Publications, U.K., 2000.

[5] C. Pellicer-Lostao, R. Lopez-Ruiz, Journal of Computational Science **1**, 24-32 (2010).

[6] S.K. Abd-El-Hafiz, Proceedings of the International Conference on Software Engineering, 88-94 (2011).

[7] S.K. Abd-El-Hafiz, Proceedings of the International Conference on Computer Software and Applications, 35-41 (2012).

[8] K. Malek, F. Gobal, Synthetic Metals **113**, 167-171 (2000).

[9] A.S. Elwakil, M. Kennedy, IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications **48**, 289-307 (2001).

[10] M.A. Zidan, A.G. Radwan, K.N. Salama, International Journal of Bifurcation and Chaos **22**, 125-143 (2012).

[11] A.G. Radwan, A.M. Soliman, A.S. Elwakil, International Journal of Bifurcation and Chaos **17**, 227-242 (2007).

[12] N.K. Pareek, V. Patidar, K.K. Sud, Image and Vision Computing **24**, 926-934 (2006).

[13] N. Singh, A. Sinha, Optics and Lasers in Engineering **48**, 398-404 (2010).

[14] S.L. Chen, T.T. Hwang, W.W. Lin, IEEE Transactions on Circuits and Systems II **57**, 996-1000 (2010).

[15] F. Pareschi, G. Setti, R. Rovatti, IEEE Transactions on Circuits and Systems I **57**, 3124-3137 (2010).

[16] G. Alvarez and S. Li, International Journal of Bifurcation and Chaos **16**, 2129-2151 (2006).

[17] A.G. Radwan, S.K. Abd-El-Hafiz, S.H. AbdElHaleem, Proceedings of the International Conference on Engineering and Technology, 1-6 (2012).

[18] C. Dong, Signal Processing: Image Communication **29**, 628-640 (2014).

[19] X. Tong, M. Cui, Signal Processing **89**, 480-491 (2009).

[20] W. Zhang, K. Wong, H. Yu, Z. Zhu, Communications in Nonlinear Science and Numerical Simulation **18**, 584-600 (2013).

[21] S.K. Abd-El-Hafiz, A.G. Radwan, S.H. AbdElHaleem, M.L. Barakat, IET Image Processing **8**, 742-752 (2014).

[22] Y. Cao, Mathematical Problems in Engineering **2013**, Article ID 728375, 13 pages (2013).

[23] J. Chen, J. Zhou, K. Wong, Z. Ji, ”Enhanced Cryptography by Multiple Chaotic Dynamics,” Mathematical Problems in Engineering **2011**, Article ID 938454, 12 pages (2011).

[24] A.N. Pisarchik, M. Zani, Physica D **237**, 638-2648 (2008).

[25] W. de Melo, S. van Strien, One-Dimensional Dynamics, Springer-Verlag, Berlin, 1993.

[26] T.-Y. Li, J. Yorke, American Mathematical Monthly **82**, 985-992 (1975).

[27] A.G. Radwan, Egyptian-Chinese Journal of Computational and Applied Mathematics **1**, 47-53 (2012).

[28] A.G. Radwan, Journal of Applied Research **4**, 163-171 (2013).

[29] A.G. Radwan, S.K. Abd-El-Hafiz, Proceeding of the IEEE International Conference on Electronics, Circuits and Systems (ICECS 2013), 653-656 (2013).

[30] K.T. Alligood, T.M. Sauer, J.A. Yorke, Chaos: An Introduction to Dynamical Systems, Springer-Verlag, New York, 1996.

[31] R. Ye, Optics Communications **284**, 5290-5298 (2011).

[32] E. B. Corrochano, Y. Mao, G. Chen, Chaos-based image encryption: Handbook of Geometric Computing, Springer, Berlin-Heidelberg, 231-265, 2005.

[33] Y. Wu, J. P. Noonan, and S. Agaian, ”NPCR and UACI randomness tests for image encryption,” Journal of Selected Areas in Teleommunications **4**, 31-38 (2011).

[34] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, E. Barker, S. Leigh, M. Levenson, M. Vangel, D. Banks, A. Heckert, J. Dray, S. Vo, A statistical test suite for random and pseudorandom number generators for cryptographic applications, Special Publication 80022, the National Institute of Standards and Technology (NIST), USA, (2001).

[35] University of Southern California, Signal and Image Processing Institute, The USC-SIPI Image Database, http://sipi.usc.edu/database/.

Salwa K. Abd-El-Hafiz received the B.Sc. degree in Electronics and Communication Engineering from Cairo University, Egypt, in 1986 and the M.Sc. and Ph.D. degrees in Computer Science from the University of Maryland, College Park, Maryland, USA, in 1990 and 1994, respectively. Since 1994, she has been working as a Faculty Member in the Engineering Mathematics and Physics Department, Faculty of Engineering, Cairo University, and has been promoted to a Full Professor in the same department in 2004. Since August 2014, she has also been working as the Director of the Technical Center for Job Creation, Cairo University, Egypt. She co-authored one book, contributed one chapter to another book and published more than 60 refereed papers. Her research interests include software engineering, computational intelligence, numerical analysis, chaos theory and fractal geometry. Prof. Abd-El-Hafiz is a recipient of the 2001 Egyptian State Encouragement Prize in Engineering Sciences, recipient of the 2012 National Publications Excellence Award from the Egyptian Ministry of Higher Education, recipient of the 2014 African Union Kwame Nkrumah Regional Scientific Award for Women in basic science, technology and innovation, recipient of several international publications awards from Cairo University and an IEEE Senior Member.

Ahmed G. Radwan (M’96–SM’12) received the B.Sc. degree in Electronics, and the M.Sc. and Ph.D. degrees in Eng. Mathematics from Cairo University, Egypt, in 1997, 2002, and 2006, respectively. He is an Associate Professor, Faculty of Engineering, Cairo University, and also with the Nanoelectronics Integrated Systems Center, Nile University, Egypt. From 2008 to 2009, he was a Visiting Professor in the ECE Dept., McMaster University, Canada. From 2009 to 2012, he was with King Abdullah University of Science and Technology (KAUST), Saudi Arabia. His research interests include chaotic, fractional order, and memristor-based systems. He is the author of more than 125 international papers, six USA patents, three books, two chapters, and h-index=17. Dr. Radwan was awarded the Egyptian Government first-class medal for achievements in the field of Mathematical Sciences in 2012, the Cairo University achievements award for research in the Engineering Sciences in 2013, and the Physical Sciences award in the 2013 International

Publishing Competition by Misr El-Khair Institution. He won the best paper awards in many international conferences as well as the best thesis award from the Faculty of Engineering, Cairo University. He was selected to be among the first scientific council of Egyptian Young Academy of Sciences (EYAS), and also in first scientific council of the Egyptian Center for the Advancement of Science, Technology and Innovation (ECASTI).

Sherif H. AbdElHaleem received the B.Sc. degree in Electronics and Communication Engineering, a Diploma in Automatic Control and the M.Sc. degree in Engineering Mathematics from the Faculty of Engineering, Cairo University, in 2002 , 2004 and 2015, respectively. From 2004 to 2015, he has been working as a professional software developer in ASIE. His research and work interests include software development, database applications, network programming, web developing and cryptography. As part of his M.Sc. work, Eng. AbdElHaleem has published several refereed papers on image encryption.