Journal of Advanced Research 10 (2018) 85–98

Contents lists available at ScienceDirect

Journal of Advanced Research

journal homepage: www.elsevier.com/locate/jare

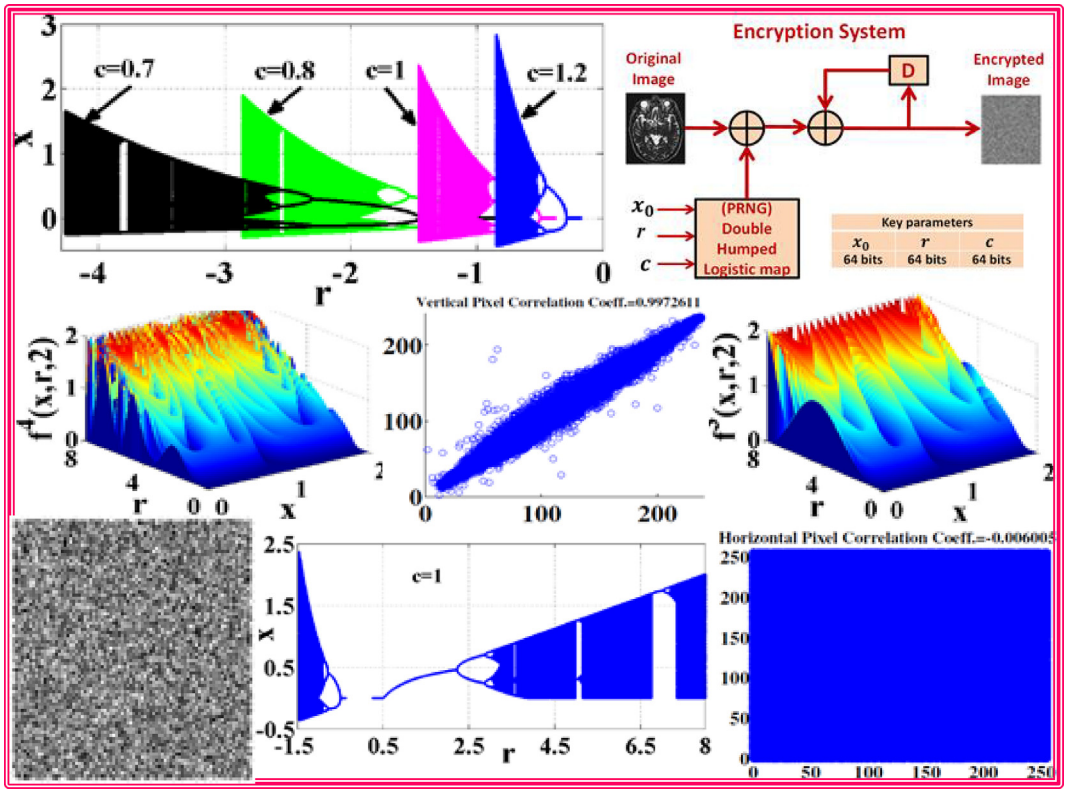
Original Article

Generalized double-humped logistic map-based medical image encryption

Samar M. Ismail [a], Lobna A. Said [b,*], Ahmed G. Radwan [c,b], Ahmed H. Madian [b,d], Mohamed F. Abu-Elyazeed [e]

[a] Faculty of IET, German University in Cairo (GUC), Cairo 11865, Egypt
[b] NISC Research Center, Nile University, Cairo 12588, Egypt
[c] Department of Engineering Mathematics and Physics, Cairo University, Cairo 12613, Egypt
[d] Radiation Engineering Department, NCRRT, Egyptian Atomic Energy Authority, 29 Nasr City, Cairo, Egypt
[e] Electronics and Communication Engineering Department, Cairo University, Cairo 12613, Egypt

GRAPHICAL ABSTRACT



Peer review under responsibility of Cairo University.

* Corresponding author.
E-mail address: l.a.said@ieee.org (L.A. Said).

https://doi.org/10.1016/j.jare.2018.01.009
2090-1232/

ARTICLE INFO

Article history:
Received 26 November 2017
Revised 15 January 2018
Accepted 24 January 2018
Available online 3 February 2018

Keywords:
Double-humped
Negative bifurcation
MLE
Image encryption
UACI
NPCR

ABSTRACT

This paper presents the design of the generalized Double Humped (DH) logistic map, used for pseudo-random number key generation (PRNG). The generalized parameter added to the map provides more control on the map chaotic range. A new special map with a zooming effect of the bifurcation diagram is obtained by manipulating the generalization parameter value. The dynamic behavior of the generalized map is analyzed, including the study of the fixed points and stability ranges, Lyapunov exponent, and the complete bifurcation diagram. The option of designing any specific map is made possible through changing the general parameter increasing the randomness and controllability of the map. An image encryption algorithm is introduced based on pseudo-random sequence generation using the proposed generalized DH map offering secure communication transfer of medical MRI and X-ray images. Security analyses are carried out to consolidate system efficiency including: key sensitivity and key-space analyses, histogram analysis, correlation coefficients, MAE, NPCR and UACI calculations. System robustness against noise attacks has been proved along with the NIST test ensuring the system efficiency. A comparison between the proposed system with respect to previous works is presented.

Introduction

Chaotic systems have gained a lot of interest for researchers lately, whether in their continuous or discrete forms. As for the discrete form, chaotic systems can be represented as maps, offering a great share in many research fields [1,2], such as theory of business cycle [3], chemistry [4], dynamics of tumor cells [5], communication [6] and encryption [7]. The discrete chaotic maps are highly sensitive to initial conditions and control parameters, which increase their randomness, unpredictability yet, being deterministic and easily reproducible. These are the main reasons why they are used in designing pseudo-random sequence generators (PRNG) for encryption purposes [8,9].

The one dimensional (1D) double humped (DH) logistic map was introduced by Coiteux [10]. It shows a double hump in its first iteration graph, and hence comes its name. The DH map has a fixed bifurcation diagram as well as a fixed chaotic range, with no control on its chaotic behavior. By using a generalization technique; through adding an extra general parameter to the equation; it gives more control to the chaotic behavior of the map facilitating the design of any map, rendering it more suitable for different applications. The generalization technique was previously introduced to generalize other logistic maps, such as the generalization of the logistic map based on fractional power introduced by Radwan [11], as well as the generalization of the logistic map in the fractional order domain by Ismail et al. [12]. The conventional DH map was previously used for PRNG in a biomedical image encryption application versus the delayed logistic map presented by Ismail et al. [13].

Medical images have become a key stone in the diagnosis and the follow up of almost all diseases. These images offer the first hand for physicians to help in patients' examination and treatment. Different technologies facilitate the existence of such medical images, as they can be generated through Computed Tomography (CT) for example, or Magnetic Resonance Imaging (MRI), or X-rays and many other techniques [14]. The patient's history is not just a plain text any more, but it also includes a lot of images documenting the development of his case to be saved in his record. These medical records are archived in a digital format and may need to be transmitted between doctors or hospitals for different clinical services via networks. Since the records contain a lot of private information about the patient, this has raised the need for developing more security techniques for this data to be transmitted and safely saved, through biomedical image encryption. Many image encryption techniques were previously used based on different technologies as the use of chaotic systems for key stream generation.

The first objective of this work is to present the generalization of the double humped logistic map, adding more control on its chaotic behavior, enabling it to be more flexible to fit in many applications. To the best of our knowledge, it is the first time to discuss the dynamics analysis of the DH map mathematically based on Cardano's formula [15]. The dynamics analysis of the proposed generalized map is discussed including fixed points, stability analysis, transient responses, bifurcation diagrams and chaotic regions. The complete bifurcation diagram, including the positive side as well as the negative side bifurcation, which is rarely discussed in literature, is also presented.

The second objective of this work is to show how different designs of the proposed generalized map are used for pseudorandom key stream generation for encryption. An image encryption system is presented based on the generalized double-humped (GDH) map. The images under test are two standard images, as well as medical images including MRI images for patients suffering from Alzheimer disease (AD) and Parkinson disease and X-ray images. Different tests are applied to the proposed encryption system, including key sensitivity and key-space analyses, histogram analysis, correlation coefficients, the Mean Absolute Error (MAE), the number of pixel change rate percentage (NPCR), the unified averaged changed intensity (UACI), and entropy calculations, as well as robustness against noise attacks, ensuring the effectiveness of the system. NIST test results are also introduced. Finally, a comparison between the presented work and other previous systems presented in literature is also detailed.

This paper first discusses the dynamics of the normal double humped logistic map. The generalized DH logistic map is then introduced including its dynamics analysis for both positive and negative sides of bifurcation. A complete overview for previously investigated image encryption systems is summarized. An image encryption system based on the proposed map is presented as an application. The security analysis of the encryption system is detailed afterwards. Comparison is introduced with previous work presented in literature and finalized by the conclusion.

Dynamics of the double humped logistic map

The one dimensional DH logistic map is so called as it exhibits a double hump in its first iteration as shown in Fig. 1(a). The DH map follows the equation:

$$x_{n+1} = r(x_n - 1)^2(1 - (x_n - 1)^2), \quad (1)$$

where r is the growth rate. Fig. 1(a) shows three successive function iterations of the DH logistic map, while Fig. 1(b) shows the 3D plots

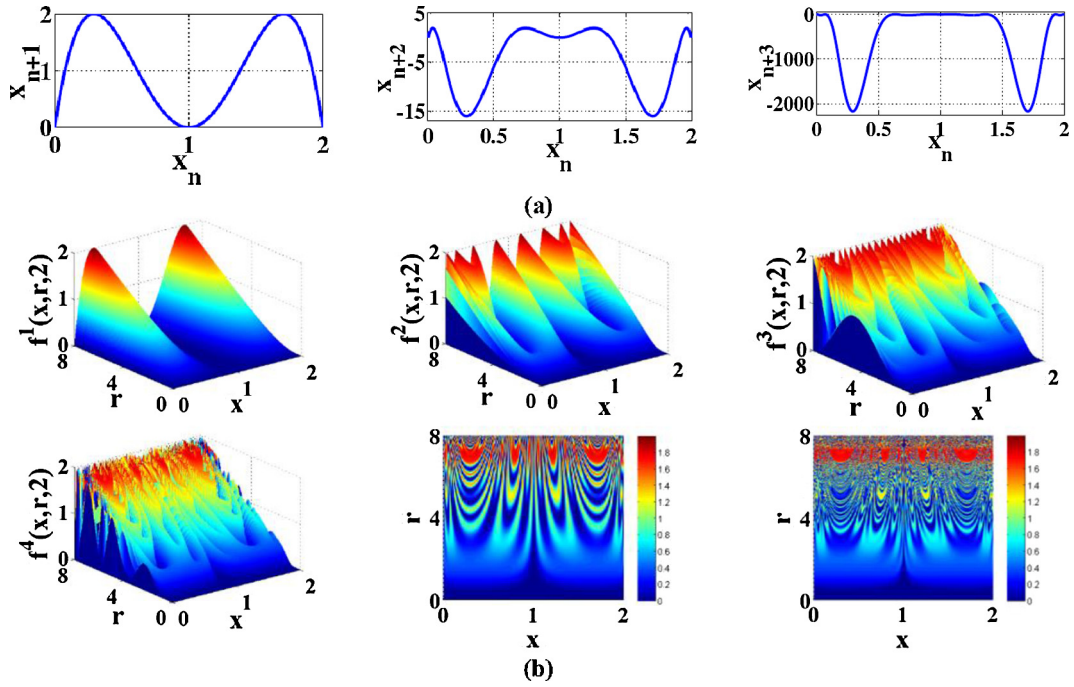


Fig. 1. DH logistic map (a) Higher order generations for r = 8 and (b) Different function iterations.

of the function iterations versus the growth parameter r, with a 2D projection view of the fifth and sixth iterations. The first iteration x_{n+1} in Fig. 1(a) has three intersection points, where $f(x) = 0$, which are $x = 0, 1$ and 2.

The minima and the maxima of f(x), are extracted by solving $f'(x) = 0$. This gives three values for x, which are $x = 1$, and $x = 1 \pm 1/\sqrt{2}$. Checking $f''(x)$ at each point gives: $f''(1) = 2r$, indicating that the point x = 1 is a minimum, $f''(1 \pm 1/\sqrt{2}) = -4r$, thus the two points $x = 1 \pm 1/\sqrt{2}$ are maxima.

The fixed points of the map (1), are calculated by equating $x^* = f(x^*, r)$, this gives the first fixed point $x_1^* = 0$, and the solution of the equation:

$$x^3 - 4x^2 + 5x + 1/r - 2 = 0. \tag{2}$$

gives the other three roots, that will depend on the value of the parameter "r".

In general, to solve an equation in the form of $ax^3 + bx^2 + cx + d = 0$, Cardano's formula [15] can be used, which says that the roots of the 3rd order degree equation are:

$$x_2 = S + T - \frac{b}{3a}, \tag{3a}$$

$$x_3 = -\frac{(S+T)}{2} - \frac{b}{3a} + \frac{i\sqrt{3}}{2}(S-T), \tag{3b}$$

$$x_4 = -\frac{(S+T)}{2} - \frac{b}{3a} - \frac{i\sqrt{3}}{2}(S-T), \tag{3c}$$

where $S = \sqrt[3]{R + \sqrt{Q^3 + R^2}}$, $T = \sqrt[3]{R - \sqrt{Q^3 + R^2}}$, $Q = \frac{3ac - b^2}{9a^2}$ and $R = \frac{9abc - 27a^2d - 2b^3}{54a^3}$.

Define a constant D as:

$$D = Q^3 + R^2 \tag{4}$$

If D > 0, then the equation has one real root and two complex conjugate roots. If D = 0, the roots are all real, with two equal roots. While for D < 0, all the roots are real and unequal.

Following Cardano's formula to solve Eq. (2), where $a = 1, b = -4, c = 5$ and $d = \frac{1}{r} - 2$, then $Q = -\frac{1}{9}$ and $R = \frac{2a-27}{54a}$. To have unequal real roots then D should be less than zero. Solving (2) for these values, gives the parameter r > 6.75.

Stability analysis of the map is studied at the fixed points. The first derivative of the function is to be calculated; the fixed points are stable if $|f'(x^*, r)| < 1$, or saddle points if $|f'(x^*, r)| > 1$. The first derivative of the function is:

$$f'(x_n, r) = r[2(x_n - 1) - 4(x_n - 1)] \tag{5}$$

At the first fixed point $x_1^* = 0$, this point is stable if $|f(0, r)| < 1$. This takes place for $r < 0.5$. It can be shown that for the range $0 < r < 0.5$, there is only one fixed point which is $x = 0$. The second range is for $0.5 < r < 6.75$, as just being proved, the function has two fixed points. Three fixed points appear at $r = 6.75$, while for $6.75 < r < 8$, the function has four fixed points. This is fully illustrated graphically in Fig. 2(a).

The Bifurcation diagram of the DH map shown in Fig. 2(b), is very similar to the conventional logistic map bifurcation diagram. The only difference that here, there are repeated bifurcations as r increases, as well as some gaps with a large one around $r = 7$. More than one chaotic region can be easily noticed in this diagram. Zooming through the diagram, when r is approximately between 6.75 and 7.0, the function converges to a single value. There appears another large gap around $r = 5$, zooming into that region, there appears a 2-cycle function. Another gap appears at around $r = 3.6$, where the function shows a 3-cycle in the range between $3.4 < r < 3.6$. All the different ranges are illustrated in Fig. 2(b) for all the regions specified. As a 3-cycle appears, the DH logistic map develops a chaotic behavior according to Sharkovsky's Theorem.

For any dynamical system, Lyapunov exponent is a quantitative measure of the sensitive dependence of this system on the initial conditions. A positive Lyapunov exponent is a chaos indicator [16], while a negative exponent indicates normal system behavior. The maximal Lyapunov exponent (MLE), for discrete maps $x_{n+1} = f(x_n)$, for an orbit starting with x_0 can be defined as

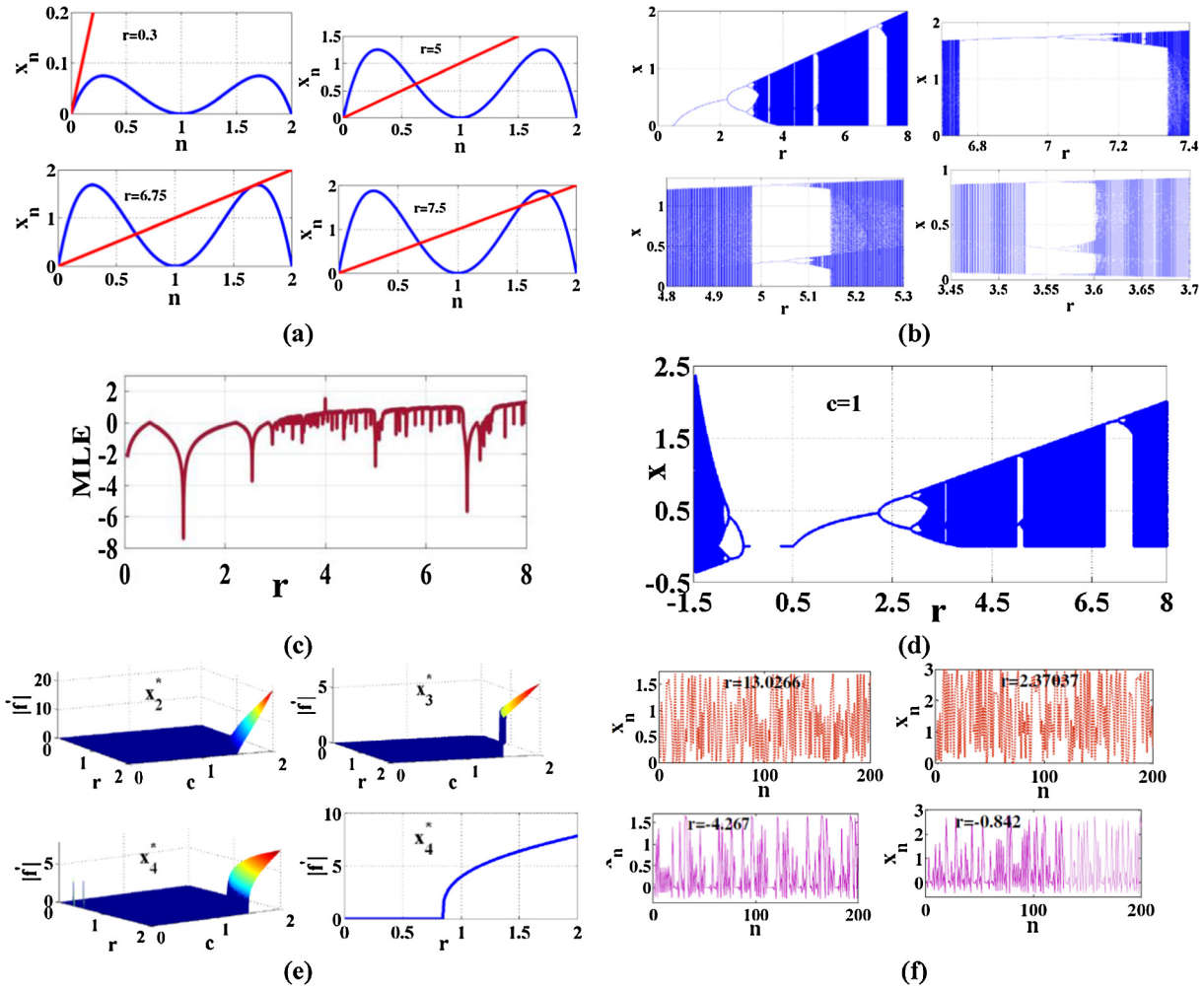


Fig. 2. The DH map (a) fixed points for different ranges of r, (b) bifurcation diagram, (c) MLE, (d) Complete bifurcation diagram for c = 1, (e) stability ranges for different r and c, and (f) transient responses for positive and negative r.

$\lambda(x_0) = \lim_{n\to\infty} \sum_{i=0}^{n-1} \frac{1}{n} \ln|f'(x_i)|$. Fig. 2(c) shows the Lyapunov exponent of the conventional DH map.

The previous discussion shows a fixed chaotic behavior of the DH map, over which no control can be done, whether controlling the chaotic range, or the value of r at which the function turns chaotic, or the value of the function at that point. To gain control on the bifurcation diagram parameters, and in order to be able to design specific maps, an extra generalized parameter can be added to the equation to make it more general and controllable through changing the value of this parameter and in consequence change the chaotic behavior of the map.

Generalized double humped (GDH) logistic map

This section introduces the generalization of the DH logistic map through adding an extra parameter c to the original equation to have:

$$x_{n+1} = r(x_n - c)^2(c^2 - (x_n - c)^2) = f(x, r, c), \tag{6}$$

where $c \in R^+$. The dynamics analysis of the proposed generalized equation is to be discussed hereby, once for the positive values of r, followed by the negative values, covering the complete bifurcation diagram of such map, shown in Fig. 2(d), for c = 1.

Positive side bifurcation

Solving to get the fixed points of the map (6), equate $x^* = f(x^*, r, c)$ as $x^* = r(x^* - c)^2(c^2 - (x^* - c)^2)$, this gives the first fixed point $x_1^* = 0$, the second fixed point is calculated by solving the equation:

$$1 + r(x^* - c)^3 - rc(x^* - c)^2 = 0. \tag{7}$$

Let $(x^* - c) = y$, thus turning into a third order equation:

$$y^3 - cy^2 + \frac{1}{r} = 0. \tag{8}$$

Using Cardano's formula as mentioned before:

$$Q = \frac{-c^2}{9}, R = \frac{\frac{-27}{r} + 2c^3}{54}, \tag{9}$$

From (4), $D = Q^3 + R^2$,

$$D = \frac{1}{4r^2} - \frac{c^3}{54r^2}, \tag{10}$$

To have unequal real roots then D should be less than zero, reaching:

$$r > \frac{13.5}{c^3} \tag{11}$$

Solving for S and T, and using Eq. (3), the roots of the generalized DH map Eq. (6) are:

$$y_2 = S + T + \frac{c}{3}, \tag{12a}$$

$$y_3 = -\frac{(S+T)}{2} + \frac{c}{3} + \frac{i\sqrt{3}}{2}(S-T), \tag{12b}$$

$$y_4 = -\frac{(S+T)}{2} + \frac{c}{3} - \frac{i\sqrt{3}}{2}(S-T), \tag{12c}$$

where the equation original roots are $x^* = y + c$, resepectively.

To calculate the maximum values of the function x, then $r(x_n - c)^2(c^2 - (x_n - c)^2) > 0$, should be solved, thus reaching:

$$x_{max} = 2c, \tag{13}$$

Solving the first derivative of the logistic equation $f'(x, r, c) = 0$, gives the critical points of the function where the function has a maximum. Three critical points can be found $x_{c_1} = 0$ and $x_{c_{2,3}} = c \pm \frac{c}{\sqrt{2}}$. For the first critical point, $f(x_{c_1}) = 0$. For the second and third critical points, $f(x_{c_{2,3}}) = r\frac{c^4}{4}$, which must be less than $x_{max} = 2c$, giving the value of the maximum value of r_{max}.

$$r_{max} = \frac{8}{c^3}. \tag{14}$$

The first derivative of the function is:

$$f'(x_n, r) = 2r[c^2(x_n - c) - 2(x_n - c)^3]. \tag{15}$$

At the first fixed point $x_1^* = 0$, this point is stable if $|f'(0, r, c)| < 1$. This takes place for $r < 0.5$. For the other three fixed points x_2^*,$x_3^*$and x_4^* which are the roots of Eq. (12); at each fixed point, a surface is drawn presented in Fig. 2(e). The graphs show the ranges at which the function is stable, $|f(x^*, r, c)| < 1$, while elsewhere it is unstable. This depends on the values of r and c for each fixed point. Fig. 2(f) shows the transient response of the GDH map for different values of the generalization parameter c ensuring chaotic behavior of the map at such values. As for the positive bifurcation side, the transient response is shown for $c = 0.85$, $r = 13.0266$, and for $c = 1.5$, $r = 2.37037$.

The effect of the generalized parameter c is shown in Fig. 3(a), where c has a zooming effect on the bifurcation diagram of the DH map according to Eqs. (13) and (14). The presence of the parameter c offers the possibility of designing any specific DH map according to a required value of x_{max} or r_{max}which gives control on the chaotic range of the map which is not possible without having this parameter. Fig. 3(b) presents 3D snapshots of the DH bifurcation diagram versus r and c.

Negative side bifurcation

The GDH map could be seen from the other side where the effect of the negative values of r on the chaotic range can be inspected following the equation:

$$x_{n+1} = -r(x_n - c)^2(c^2 - (x_n - c)^2). \tag{16}$$

The critical points are calculated by solving the equation $f'(x, r, c) = -r[2c^2(x_n - c) - 4(x_n - c)^3] = 0$. This gives three critical points $x_{c_1} = 0$ and $x_{c_{2,3}} = c \pm \frac{c}{\sqrt{2}}$. For the first critical point, $f(x_{c_1}) = 0$. For the second and third critical points, $f(x_{c_{2,3}}) = -r\frac{c^4}{4}$, which is equal to x_{min}. Solving for $f(x_{min}) = x_{max}$, the expression of x_{max} could be reached to be equal to:

$$x_{max} = \frac{r^2}{2}c^7\left(\frac{r^3}{128}c^9 + \frac{r^2}{8}c^6 + \frac{5r}{8}c^3 + 1\right) \tag{17}$$

Substituting in $x_{max} = f(x_{max})$, r_{max} value could be calculated numerically from the following equation:

$$rc^3\left[\frac{1}{256^3}r^{15}c^{45} + \frac{3}{16(256^2)}r^{14}c^{42} + \frac{63}{16(256^2)}r^{13}c^{39} + \frac{95}{131072}r^{12}c^{36} + \frac{363}{65536}r^{11}c^{33} + \frac{455}{16384}r^{10}c^{30} + \frac{369}{4096}r^9c^{27} + \frac{43}{256}r^8c^{24} + \frac{1}{16}r^7c^{21} - \frac{33}{64}r^6c^{18} - \frac{315}{256}r^5c^{15} - \frac{11}{16}r^4c^{12} - \frac{25}{16}r^3c^9 - \frac{5}{2}r^2c^6 - 2\right] - 1 = 0 \tag{18}$$

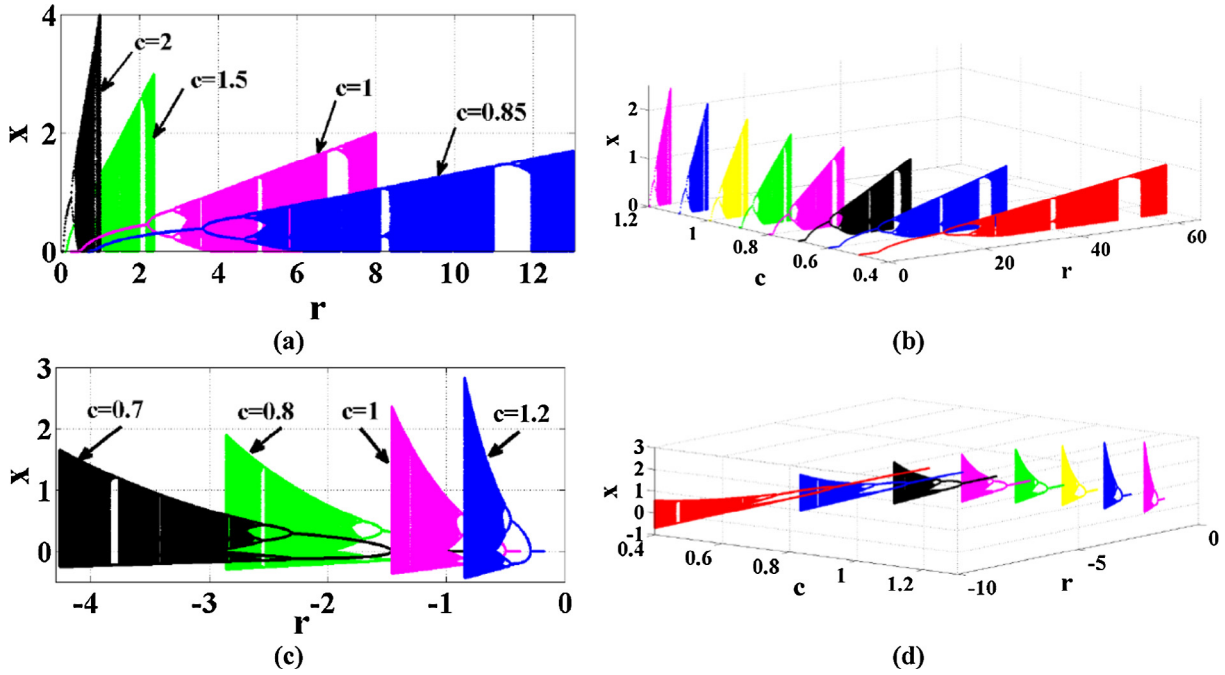


Fig. 3. The DH map bifurcation diagram (a) different values of c for +r, (b) 3D snapshots versus c for +r, (c) for different values of c for −r, (d) 3D snapshots versus c for −r.

Fig. 2(f) shows the function variations of the GDH map for different values of c, versus n, for $c = 0.7$, $r = -4.267$ and $c = 1.2$, $r = -0.842$. The effect of the generalized parameter c on the negative bifurcation diagram is shown in Fig. 3(c), for different values of c, while Fig. 3(d) shows 3D snapshots of the bifurcation diagrams showing the zooming effect of c on the map.

An application: image encryption system

Overview on encryption systems

There were previous encryption systems presented in literature based on the chaos theory such as the one introduced by Pisarchik et al. [17], proposing direct encryption and decryption of digital images with chaotic map lattices. The image encryption algorithm was based on many logistic maps in cascaded loops. While a secure cryptosystem was presented for color images by Pisarchik and Zanin [18], it was based on chaotically coupled chaotic maps, depending on mixing conventional logistic maps, offering good confusion and diffusion properties. A Partial encryption chaos-based system was presented by Soma and Sen to encrypt gray scale images [19]. The algorithm depended on bit plane decomposition of the original image then encrypted using pseudorandom binary number generator based on couple tent map. Telem et al. presented a robust gray image encryption system using conventional logistic map and artificial neural network [20]. The initial conditions of the logistic map were derived using an external secret key. A chaos-based symmetric image cryptosystem employing the Arnold cat map for bit-level permutation and the logistic map for diffusion, unlike the other systems based on pixel-level permutation, was presented by Zhu et al. [21]. While Pareek et al. proposed, a simple encryption algorithm for gray images based on diffusion and substitution processes, offering high encryption rate [22]. Moreover, a simple encryption system using fractional-order logistic map for key generation was presented by Ismail et al. [12], having larger key space and extra degree of freedom using the fractional-order parameter in the key. A stream cipher system was also proposed by Ismail et al. [13], using delayed version of the logistic map comparing it to the same system while using the double-humped logistic map versus different security analysis aspects. Abd-El-Hafiz et al. presented the mathematical aspects of a generalized sine map with arbitrary powers and scaling factor, and two image encryption applications were introduced based on the generalized sine map [23]. The first system only performed pixel value substitutions, while the second system performed both permutations and substitutions.

Based on Lorenz chaotic system and perceptron model in a neural network, a chaotic image encryption system was proposed by Wang et al. [24]. Using the deoxyribonucleic acid (DNA) coding, a novel confusion and diffusion method for image encryption was proposed by Liu and Wang [25]. The chaotic map used was the piecewise linear chaotic map (PWLCM), and each nucleotide was transformed into its base pair using the DNA complementary rule. Also, an image encryption scheme was introduced by Wang et al. [26], depending on DNA sequence operations and the pseudorandom sequences produced by the spatiotemporal chaos system which was coupled map lattice (CML). Moreover, based on the mixed linear-nonlinear coupled map lattices, a new image encryption algorithm was presented by Zhang and Wang [27,28], where bit-level pixel permutation was used allowing the lower and higher bit planes to permute mutually without any extra storage space. Wang et al. also proposed a new block image encryption scheme based on hybrid chaotic maps (Arnold cat map) and dynamic random growth technique [29]. A stream-cipher algorithm based on one-time keys and robust chaotic maps for colored image encryption was presented by Liu and Wang [30]. The piecewise linear chaotic map was used to generate a pseudo-random key sequence. They also presented a bit-level permutation and high-dimension chaotic map was used to encrypt color image [31]. The scrambling mapping was generated by PWLCM, and then the Chen system was employed to confuse and diffuse the red, green and blue components, simultaneously. Some other encryption systems were also presented in literature [32–39] using chaotic maps whether for grayscale or colored images.

Proposed system

The employed GDH map, being a chaotic map, can be used for pseudorandom number key generation (PRNG) to be used in an image encryption system to secure biomedical images. The block diagram of the proposed encryption system is shown in Fig. 4(a). The key stream used for encryption consists of the GDH parameters, which are the map initial value x_0, the growth rate r and the generalization parameter *c*. The pseudo random numbers are generated by recursively solving the map to get (x). For each iteration, the 8 Least Significant Bits of the new value of (x) is xored with a new pixel from the image to be encrypted. The output is to be xored again with a delay block output, which gives a 0 output for the first iteration only. Then in the successive iterations, it provides the previously encrypted pixel. This process is repeated for all the image pixels to reach the final encrypted image. Fig. 4(b) shows a set of six test images used for the encryption system evaluation, with different sizes. The test image could be any medical image including MRI, CT or X-ray images as well as any natural image. Two standard images are traditionally used in the image processing field, which are Lena and Barbara. The other four are medical images, which are a Lung-XRAY, an MRI image of a patient suffering of Alzheimer disease (AD), a Parkinson disease MRI and finally a knee sagittal MRI image.

Table 1 shows the encrypted versions of the input images for different values of *c*, for both positive and negative bifurcation sides. For each case, a wrong decrypted image is presented as well; this is in response to adding a value of 0.001% of the corresponding *c* in the decryption process, compared to the value used in the encryption process. From the results shown, the image cannot be restored, which represents a very high sensitivity of the key generator to the generalization parameter.

Security analysis

The efficiency of any encryption algorithm could be defined by using some numerical security analyses. In this section, the performance analysis measures like key space analysis and parametric sensitivity analysis, histogram analysis, uniformity variance analysis, correlation analysis, entropy as well as differential attacks analyses are presented to ensure the efficiency of the proposed system. The images used in security analyses of the cryptosystem proposed is the set of two standard images (Lena and Barbara) as well as some medical images.

Pixel correlation analysis

The correlation test is one of the frequently used methods for testing an encryption system, where the correlation is calculated by [7]:

$$C_{XY} = \frac{cov(X,Y)}{\sqrt{D_X}\sqrt{D_Y}}, \tag{19}$$

where cov(X, Y) calculates the covariance between X and Y and D_X is the variance of X. Since the image pixels are highly correlated to each other, a decrease in the correlation coefficients of the horizon-

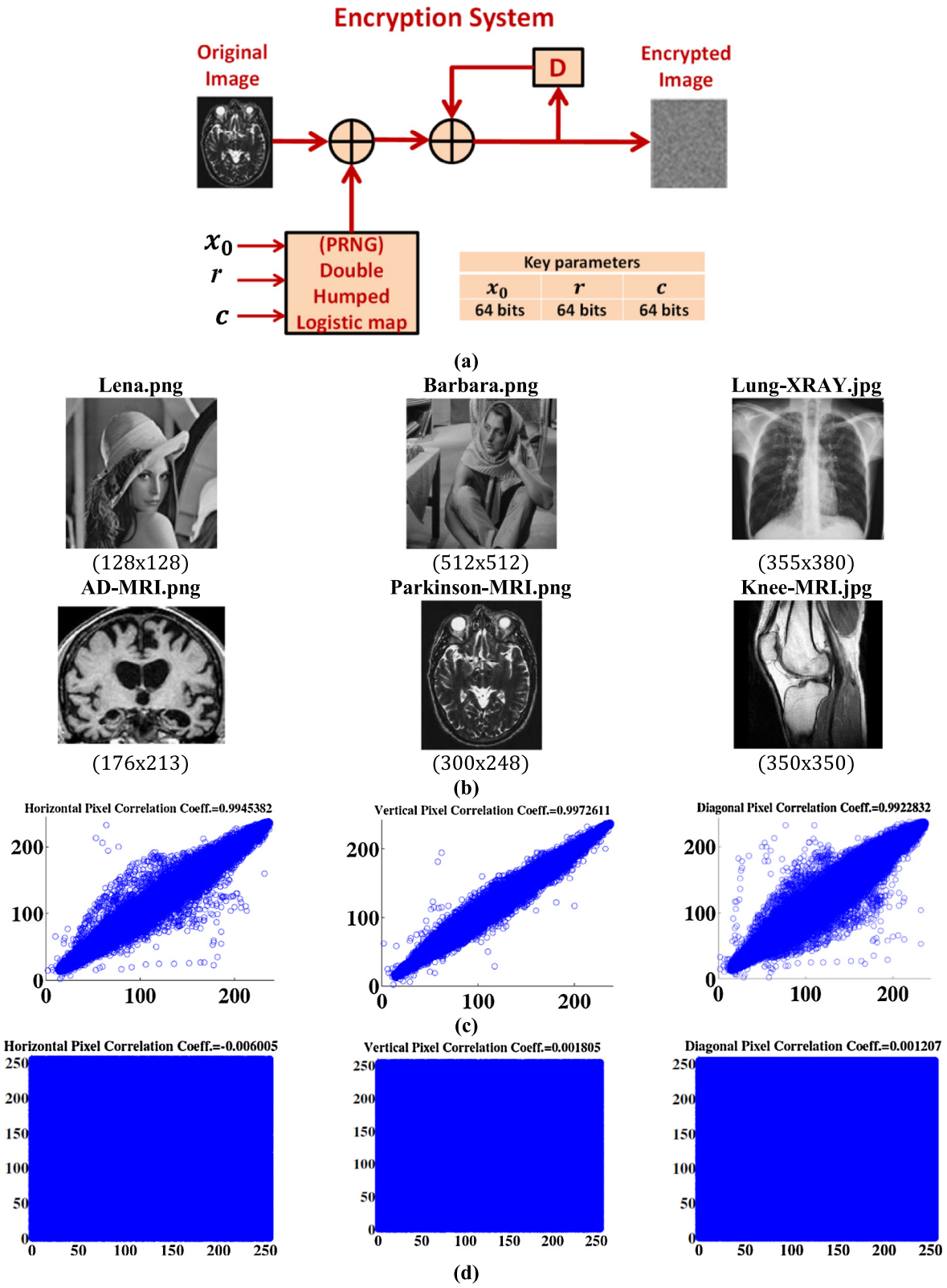


Fig. 4. (a) Image encryption system block diagram, (b) Test images used for encryption, Pixel correlation diagrams of (c) Lung-Xray image and (d) its encrypted image for $+r$ and c = 1.5.

tal, vertical, and diagonal pixels of the image is an indication of the encryption system strength. Table 2 presents the correlation coefficients for the all the source images and the encrypted images in details, for different values of *c*, for both positive and negative bifurcation sides, showing very low correlation coefficients. Fig. 4(c) and (d) presents the correlation results for the Lung-X-ray image and its encrypted version for positive r with c = 1.5 GDH map used for key generation.

Table 1
Encrypted and wrong decrypted images with different values of parameter c for $\pm r$.

	Positive bifurcation $+r$						Negative bifurcation $-r$					
	$c = 0.85$		$c = 1$		$c = 1.5$		$c = 0.7$		$c = 1$		$c = 1.2$	
	Encrypt Image	Wrong Decrypt	Encrypt Image	Wrong Decrypt	Encrypt Image	Wrong Decrypt	Encrypt Image	Wrong Decrypt	Encrypt Image	Wrong Decrypt	Encrypt Image	Wrong Decrypt
Lena												
Barbar												
Lung-XRAY												
AD-MRI												
Parkin-MRI												
Knee-MRI												

Key space analysis

The key space should be large enough to resist brute-force attacks. The key consists of three control parameters, the initial condition x_0, the growth rate r and the generalization parameter c. Each parameter consists of 64 bits, rendering the key length equal to 192 bits long, with a precision of 10^{-16}. The key space size employed in this work is $2^{192} = 10^{57}$.

Key sensitivity analysis

Chaotic maps are known that they are highly sensitive for any small change in the initial conditions or the system parameters. Sensitivity analysis is done for every parameter of the key generator used for encryption. Changing a very small perturbation of $\Delta = \pm 0.001\%$ of the parameter under test, the encrypted image should be no longer restored to the original image. This indicates how the system is highly sensitive to very small changes in the key parameters insuring the encryption system high security level. Fig. 5 shows the resultant decrypted images for Lena image, in case there is a change of $\Delta = \pm 0.001\%$ of the map parameters r, c or the initial condition x_0 for both positive and negative bifurcation sides of the map. For the negative side, for example, the initial condition $x_0 = 0.1$, is once taken as 0.10001 and another time 0.099999, with only 0.00001 difference, while fixing $r = -1.46, c = 1$. The images cannot be decrypted to Lena again; this is due to the high sensitivity for the generalized logistic map proposed for generating the key.

Fig. 6(a) and (b) show two ciphered Lena image for parameters values $x_0 = 0.1$,$r = 2.37037$, while changing $c = 1.5$ and $c + \Delta = 1.499985$, respectively, with only 0.00001 difference. The two ciphered images are completely different with the difference image shown in Fig. 6(c). The simulation analysis show that the algorithm presented is key-sensitive, where a minor change in any of the key parameters results in a significant change in the ciphered results.

The decrypted images are also being compared quantitatively, by measuring the correlation coefficient between two decrypted images upon having a slight change in the decryption key compared to the encryption key used for encryption. The case under study is the decrypted images shown in Fig. 5 for the negative bifurcation side, including images in Fig. 5(g), (h) and (i), where the decryption key has a slight change in the initial condition x_0, in the growth rate r and in the generalization parameter c, respectively. Table 2 shows that there is no clue about the plain image could be found upon having a little change in the key. The correlation coefficient calculated for each case is approaching zero. These results confirm the proposed system effectiveness.

To have a quantity analysis of any key, mutual information (MI) calculation is employed to evaluate the key sensitivity of any two ciphered images for example (y and z), which are encrypted versions by different keys on the same plaintext image, upon changing a very small $\Delta = \pm 0.001\%$ of the key parameters r, c or x_0. The higher the sensitivity of the key, the lower the value of the mutual information of (y and z). The mutual information is calculated following the equation:

$$MI = Hy + Hy - h_{yz}, \tag{20}$$

where Hy is the entropy of the ciphered image y, Hz is the entropy of the ciphered image z, and h_{yz} is the mutual entropy between both images. For each key parameter, the MI is measured while fixing the other parameters, listed in Table 2. The plaintext images used are the standard images Lena, Barbara and Cameraman of extension '.bmp'. The information shared between the two ciphered images is close to zero, indicating the high key sensitivity of the system.

Histogram analysis

The distribution of information of pixel values inside any image can be shown using histogram analysis [7]. If the histogram of the image after being encrypted is uniformly distributed, this is considered an indication of the encryption system strength. Table 3

Table 2
Correlation coefficients and key sensitivity analysis.

		Positive bifurcation $+r$								
		Lena			Barbara			Lung-X-ray		
		H	V	D	H	V	D	H	V	D
Source image		0.8915	0.9494	0.8699	0.9232	0.9744	0.9186	0.9945	0.9973	0.9923
ENC	c = 0.85	0.0082	0.0025	0.0027	0.0076	0.0029	0.0002	0.0035	0.0002	−0.0013
	c = 1	−0.0005	−0.0019	0.0003	−0.0006	−0.0018	−0.0012	0.0035	0.0002	−0.0012
	c = 1.5	−0.0013	0.0080	−0.0094	−0.0013	−0.0047	0.0007	−0.0060	0.0018	0.0012
		AD-MRI			Parkinson-MRI			Knee-MRI		
		H	V	D	H	V	D	H	V	D
Source image		0.9627	0.9512	0.9223	0.9047	0.9432	0.8572	0.9746	0.9873	0.9690
ENC	c = 0.85	0.0075	−0.0048	0.0039	0.0103	−0.0031	−0.0029	0.0052	0.0039	−0.0011
	c = 1	0.0075	−0.0059	−0.0041	−0.0026	0.0057	0.0012	−0.0042	−0.0045	−5.0682e−04
	c = 1.5	−0.0022	0.0025	0.0036	0.0004	0.0027	−0.0020	−0.0032	0.0036	−0.0032
		Negative bifurcation $-r$								
		Lena			Barbara			Lung-X-ray		
		H	V	D	H	V	D	H	V	D
Source image		0.8915	0.9494	0.8699	0.9232	0.9744	0.9186	0.9945	0.9973	0.9922
ENC	c = 0.7	0.0110	−0.0054	0.0018	0.0115	0.0016	−6.7028e−04	0.0035	0.0018	0.0014
	c = 1	0.0133	−0.0154	−0.0032	0.0121	0.0023	8.3084e−04	−0.0014	0.0021	−3.9151e−04
	c = 1.2	−0.0076	0.0012	0.0019	0.0053	−5.8486e−04	−1.6640e−04	0.0022	−0.0012	0.0018
		AD-MRI			Parkinson-MRI			Knee-MRI		
		H	V	D	H	V	D	H	V	D
Source image		0.9627	0.9512	0.9223	0.9047	0.9432	0.8572	0.9746	0.9873	0.9690
ENC	c = 0.7	0.0121	0.0070	−0.0014	0.0223	0.0020	1.0177e−04	0.0085	0.0021	0.0018
	c = 1	0.0100	−0.0050	0.0086	0.0252	6.1136e−04	−0.0027	0.0083	−0.0011	0.0012
	c = 1.2	−0.0098	0.0026	−0.0065	0.0073	8.5364e−04	0.0013	0.0075	0.0065	0.0017

Correlation coefficients between different decrypted images shown in Fig. 5

Decrypted images compared	Correlation coefficient
Fig. 5(g) and (h)	0.0065
Fig. 5(g) and (i)	0.0080
Fig. 5(h) and (i)	0.0072

Mutual information among key parameters

	Positive bifurcation $+r$		
	$x_0 = 0.1$	$r = 8$	$c = 1$
Lena	0.1892	0.1921	0.1912
Barbara	0.1920	0.1888	0.1899
Cameraman	0.0208	0.0210	0.0209
Average	0.1340	0.1339	0.1340

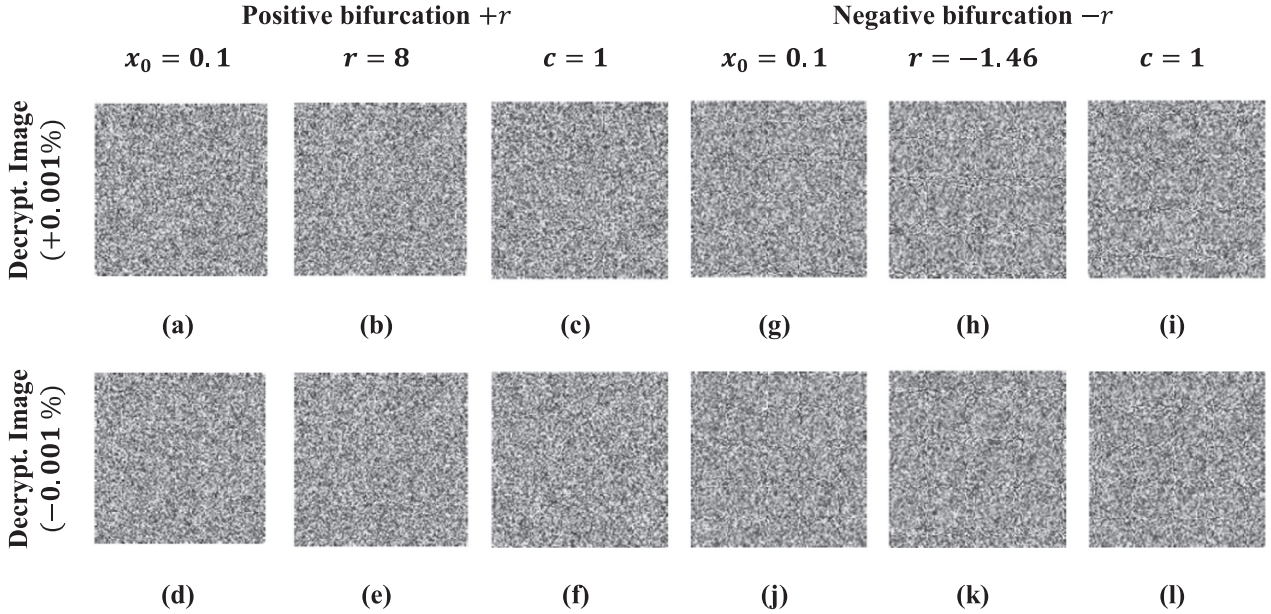


Fig. 5. Sensitivity analysis to system parameters.

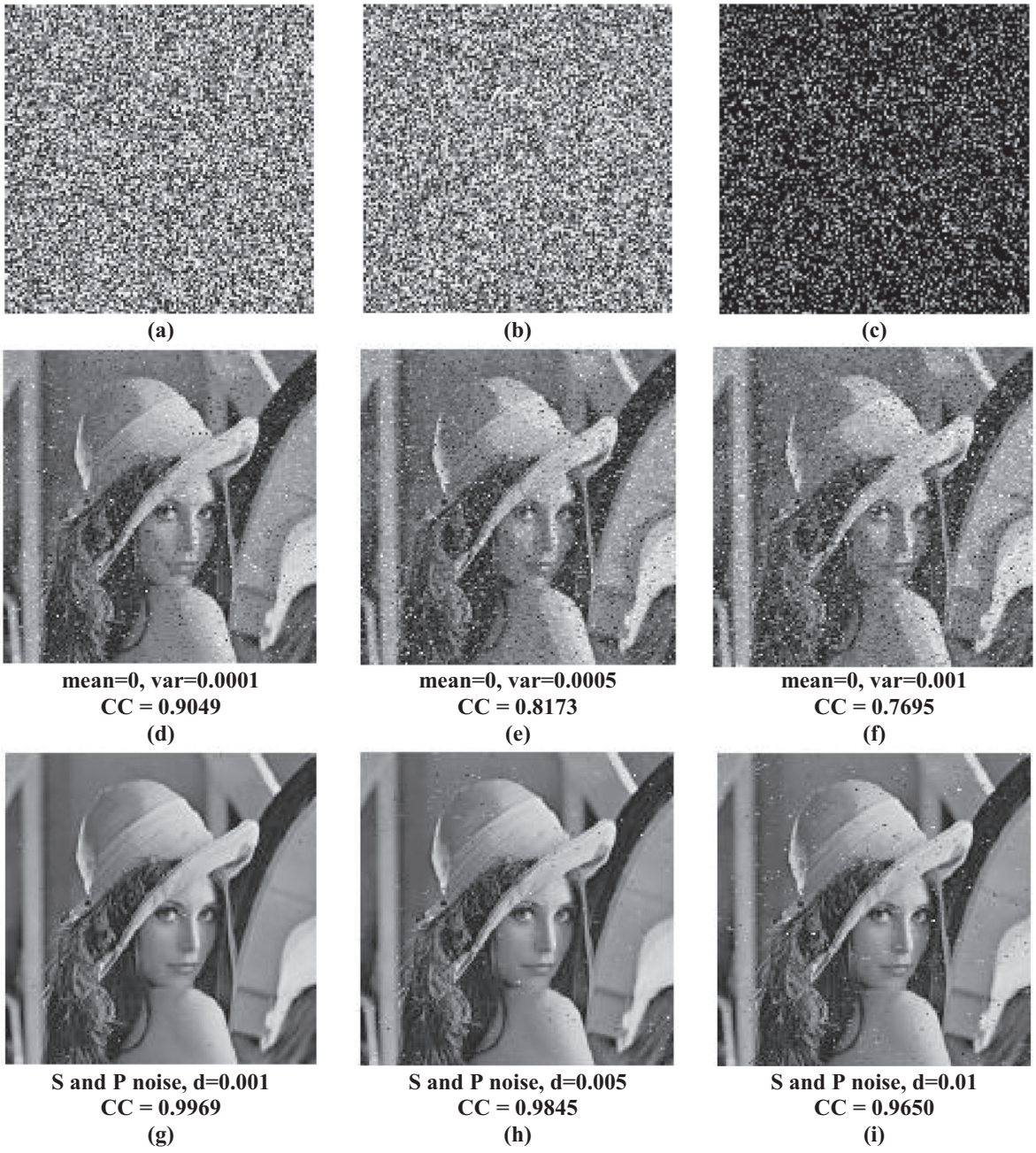
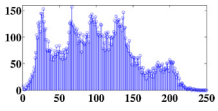
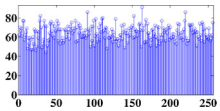
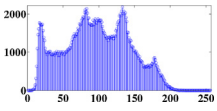
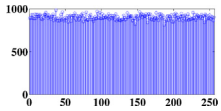
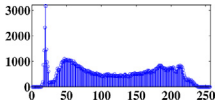
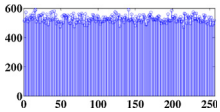
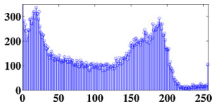
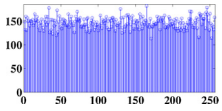
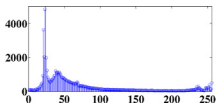
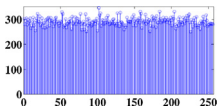
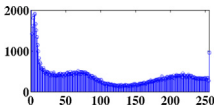
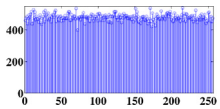


Fig. 6. Key sensitivity of parameter c (a) ciphered image c, (b) ciphered image $c + \Delta$ and (c) difference between (a) and (b), Deciphered images of noisy plain-images with Gaussian noise in (d), (e) and (f) and with salt and pepper noise in (g), (h) and (i).

shows the histogram of the plain images as well as the ciphered images for $+\boldsymbol{r}$ at $c = 1$, $x_0 = 0.1$ and $r = 8$, displaying flat histograms for the images after encryption. The histograms of the ciphered images show completely uniform and significantly different than the fluctuating histograms of the plain images, which is important in resisting any statistical attack. The uniformity of the ciphered image gray scale, infers that no useful information could be retrieved upon performing any statistical attack on the ciphered image.

The uniformity of the histogram analysis can be quantified by measuring the minimum value, the maximum value as well as the variance of the histogram of the plain-image. Moreover, the minimum value, the maximum value as well as the variance of the histogram of the ciphered-image are calculated. The efficiency of the system is validated when comparing the range of the minimum and maximum values of the plain-image versus the corresponding range of the ciphered image, calculated as (maximum-minimum). It is very clear that the ciphered-image, having an approximately flat histogram, has a very small range in comparison with the plain-image fluctuating histogram. Also, the variance values calculated for the plain-image histogram is much more less than the variance value calculated for the ciphered-image histogram, validating the uniformity of the histogram analysis of the proposed cryptosystem. These results of the variance, minimum-maximum range values are enumerated in Table 3, for different standard images of different sizes. Discussing one case for example, for plain-image Lena of size 512×512, the range between the minimum and maximum values is 2723, while the

Table 3
Histogram of the original and the encrypted images for +r and variance analysis.

Lena		Barbara	
			
Lung-X-ray		**AD-MRI**	
			
Parkinson-MRI		**Knee-MRI**	
			

Variance analysis of the uniformity of ciphered images

		Plain-Image				Ciphered Image			
Test Image	Size	Min	Max	Range	Variance	Min	Max	Range	Variance
Lena	256 × 256	0	584	584	3.0708e+04	205	308	103	281.2314
Lena	512 × 512	0	2723	2723	6.3473e+05	947	1127	180	976.8627
Baboon	256 × 256	0	964	964	1.0790e+05	213	300	87	267.2078
Baboon	512 × 512	0	2708	2708	7.5246e+05	910	1110	200	1025
Barbara	512 × 512	0	2217	2217	3.8369e+05	935	1108	173	942.6353
Camman	256 × 256	0	2596	2596	1.6190e+05	213	306	93	257.1686

range of the corresponding ciphered-image is only 180. Moreover, for the same case, the variance of the plain-image is found to be $6.3473e+05$, while the variance of the ciphered image is only 976.8627, validating the uniformity of the flat histogram obtained after encryption.

Entropy analysis

Information entropy is one of the most important parameter for measuring randomness. The image information content can be measured using the entropy H, if the probability distribution of the image is known. For a random variable with a probability distribution P_k, the entropy can be calculated for n values as follows [7]:

$$H = -\sum_{k=1}^{n} P_k \log_2(P_k). \tag{21}$$

The entropy is measured in bits. Ideally if H is equal to 8, this means that the information is totally random. The entropy values presented are approximately 8 which validates the encryption system efficiency. Table 4 shows the entropy results for all the set of images, for both positive and negative bifurcation sides versus different values of the generalization parameter *c*.

Classical types of attacks

There are four types of classical cryptanalytic attacks based on the amount of information known to the cryptanalyst, and these types are:

- **Ciphertext only:** In this method, the opponent has access to a string of ciphertext. He does not have access to corresponding plaintext.
- **Known plaintext:** In this method, the opponent knows a string of plaintext, and the corresponding ciphertext. Using this information, it is required to decrypt the rest of the ciphertext.
- **Chosen plaintext:** In this method, the opponent can access the encryption device and chooses a string of plaintext and construct its corresponding ciphertext string. By this information, it is easy to determine the encryption key.
- **Chosen ciphertext:** In this method, the opponent can access the decryption device and chooses a string of ciphertext and construct its corresponding plaintext string.

The chosen plaintext attack is the most powerful attack and if a cryptosystem can resist this attack, it can resist other types of attack as previously reported [34].

Differential attacks

Differential attacks are some measurements done to confirm the security of a given encryption system [7]. Three common measures of the differential attacks are the Mean Absolute Error (MAE), the number of pixel change rate percentage (NPCR) and the unified averaged changed intensity (UACI). Conventionally, high MAE, NPCR and UACI values are usually interpreted as a high resistance of the encryption system to differential attacks. The absolute change between the encrypted image E and the source image *S*, measured by the MAE, is defined as [7]:

$$MAE = \frac{1}{WxH}\sum_{i=1}^{H}\sum_{j=1}^{W}|E(i,j) - S(i,j)|, \tag{22}$$

where W and H are the width and height of the source image (*S*). The differential attacks study the relation between the normal encrypted image (E1) and another encrypted image under the effect of changing one pixel in the original image (E2). E (i, j) is the pixel value at the location (i, j) for the corresponding image E.

The percentage of the number of pixel change between the two images (E1) and (E2) is measured by NPCR, calculated as [7,40]:

$$NPCR = \frac{1}{WxH}\sum_{i=1}^{H}\sum_{j=1}^{W}D(i,j) \times 100\%, \tag{23a}$$

Table 4
Differential Attacks analysis results for different images.

	Positive bifurcation $+r$					Negative bifurcation $-r$				
	c	Entropy	MAE	NPCR (avg)	UACI (avg)	c	Entropy	MAE	NPCR (avg)	UACI (avg)
Lena	0.85	7.9885	77.7790	75.6256	34.9441	0.7	7.9871	77.2129	75.62561	35.0643
	1	7.9889	77.0094	75.6256	34.9527	1	7.9892	77.8253	75.62561	34.8779
	1.5	7.9907	78.1754	75.6256	34.8651	1.2	7.9888	77.4624	75.6256	34.9782
Barba	0.85	7.9993	76.2103	75.5000	31.4231	0.7	7.9992	76.2984	75.5000	31.4492
	1	7.9992	76.2310	75.5000	31.4618	1	7.9992	76.1708	75.5000	31.4732
	1.5	7.9992	76.2261	75.5000	31.4732	1.2	7.9993	76.1374	75.5000	31.4442
Lung	0.85	7.9987	81.2101	75.5000	31.8133	0.7	7.9986	81.2617	75.5000	31.7949
	1	7.9985	81.0042	75.5000	31.7341	1	7.9987	81.1266	75.5000	31.7597
	1.5	7.9987	81.1531	75.5000	31.8026	1.2	7.9986	81.0291	75.5000	31.7571
AD	0.85	7.9954	87.5625	75.5575	29.7107	0.7	7.9946	88.3132	75.5575	29.7632
	1	7.9945	87.7781	75.5575	29.7555	1	7.9957	87.84262	75.5575	29.7861
	1.5	7.9946	87.5776	75.5575	29.7563	1.2	7.9956	88.07746	75.5575	29.7857
Parkn	0.85	7.9978	94.3581	75.5000	29.4095	0.7	7.9975	93.83713	75.5000	29.3711
	1	7.9977	94.0663	75.5000	29.3684	1	7.9977	93.94367	75.5000	29.3771
	1.5	7.9981	94.3686	75.5000	29.4023	1.2	7.9977	94.46904	75.5000	29.3771
Knee	0.85	7.9986	100.0917	75.5000	24.8565	0.7	7.9984	100.1994	75.5000	24.8939
	1	7.9988	99.8536	75.5000	24.8268	1	7.9986	100.1060	75.5000	24.8278
	1.5	7.9983	100.1856	75.5000	24.9201	1.2	7.9984	100.0359	75.5000	24.8522

$$D(i,j) = \begin{cases} 0 & E1(i,j) = E2(i,j) \\ 1 & E1(i,j) \neq E2(i,j) \end{cases}. \tag{23b}$$

The term UACI measures the average light intensity of the differences between the two images (E1) and (E2), and it is calculated as [7,40]:

$$UACI = \frac{1}{WxH}\sum_{i=1}^{H}\sum_{j=1}^{W}\frac{|E1(i,j) - E2(i,j)|}{255} \times 100\%. \tag{24}$$

Table 4 shows the differential Attacks analysis results for the images for the three cases of c. The NPCR and the UACI results are calculated as the average of 50 trials.

An efficient cryptosystem should be sensitive to the secret keys as was shown in the key sensitivity analysis as well as the plain-text. For all the images under test and for all the cases whether positive or negative bifurcation maps, in each time two ciphered images are obtained upon changing only one bit in the plain-image, and measure the NPCR of the resultant ciphered images. The values of the NPCR presented in Table 4 shows that upon changing only one pixel in the plain-image, different ciphered images are obtained; confirming that the cryptosystem proposed is sensitive to changing plain image and can resist the chosen plain-text attack [34].

Moreover, the closer the UACI values to the values presented in Wu et al. [40], the more the effectiveness of the cryptosystem in resisting differential attack [34]. The UACI value depends on the size of the image as can be seen in the table and as reported earlier by Wu et al. [40].

Robustness against noise

The electronic transmission of ciphered images from transmitter to receiver, may suffer some additive noise in practical life, which may cause an inevitable error leading to difficulties in decryption, and this point is very important specially in medical images transfer through doctors and hospitals. If the cryptosystem is noise sensitive, then a small change in the ciphered image due to noise addition may hinder the original image restoration after decryption [25,39]. The system proposed is being tested to applying white Gaussian noise to the ciphered image of Lena, with different variances. This type of noise is a reasonable assumption of randomness caused by real physical channels, and the random numbers of this noise is uniformly distributed through the ciphered image. The results shown in Fig. 6(d–f) show how much the cryptosystem proposed is robust against noise. Moreover, the same image Lena, is being tested while adding Salt and Pepper (S and P) noise to the ciphered image, with different densities, and the decrypted image of each case is shown in Fig. 6 also confirming the system efficiency against noise attacks. The correlation coefficients (CC) between the noiseless decrypted image and the noisy decrypted image are enumerated for each noisy case in Fig. 6. If the deciphered image is very close to the original whether visually or numerically through the measurement of the correlation coefficients, i.e. close to 1, this proves that the system is noise immune, which is proved in the reported results, as the decrypted images still maintain the overall information of the original image.

NIST statistical test

The NIST statistical test suite provides typical tests to measure the randomness of the encrypted image [41]. In this evaluation, two standard images were used "Lena" and "Man" with resolution 1024×1024 and four different combinations of the generalized DH map were applied. Cases 1 and 2 are for positive bifurcation side of the GDH map, with values $(c = 1, r = 8)$, and $(c = 1.5, r = 2.37037)$ respectively. On the other hand, cases 3 and 4 are for negative bifurcation side of the GDH map with values $(c = 0.7, r = -4.267)$, and $(c = 1.2, r = -0.842)$ respectively. The test results are reported in Table 5, and the success in all the 15 tests further asserts the randomness of the encrypted images.

Discussion and comparisons

This section presents a comparison for the proposed system with previously introduced systems in literature. For the sake of fair comparisons, only the standard images with different sizes are employed in this section. The comparison includes key space analysis, sensitivity analysis, entropy analysis, and correlation coefficients calculations. The key space size employed in this work is $2^{192} = 10^{57}$ which is more than the key space presented elsewhere [22,32–34] as being compared in Table 6. Thus, the encryption system used in this work can resist all kinds of brute force attacks having a large enough key space.

Table 5
NIST test.

Sample NIST results for encrypted images (1024 × 1024)								
Test	Case 1		Case 2		Case 3		Case 4	
	PV	PP	PV	PP	PV	PP	PV	PP
Frequency	√	1.000	√	1.000	√	1.000	√	1.000
Block Frequency	√	1.000	√	1.000	√	1.000	√	1.000
Cumulative Sums	√	1.000	√	1.000	√	1.000	√	1.000
Runs	√	1.000	√	1.000	√	1.000	√	1.000
Longest Run	√	1.000	√	1.000	√	1.000	√	1.000
Rank	√	1.000	√	1.000	√	1.000	√	1.000
FFT	√	1.000	√	1.000	√	1.000	√	1.000
Non Overlapping Template	√	0.994	√	0.992	√	0.992	√	0.995
Overlapping Template	√	1.000	√	1.000	√	1.000	√	1.000
Universal	√	1.000	√	1.000	√	1.000	√	1.000
Approximate Entropy	√	1.000	√	1.000	√	1.000	√	1.000
Random Excursions	√	1.000	√	1.000	√	0.975	√	1.000
Random Excursions Variant	√	1.000	√	1.000	√	0.989	√	0.972
Serial	√	1.000	√	1.000	√	1.000	√	0.938
Linear Complexity	√	1.000	√	1.000	√	1.000	√	1.000
Final Result	Success		Success		Success		Success	

Table 6
Comparison between previous encryption systems and this work.

Key space comparison with existing algorithms							
Algorithms	Ref [32]	Ref [22]	Ref [35]	Ref [21]	Ref [33]	Ref [34]	This work
Key space	10^{30}	10^{38}	10^{38}	10^{42}	10^{56}	10^{56}	10^{57}

Correlation Coefficients comparison for Lena										
		Ciphered Image								
Directions	Plain-Image	[21]	[24]	[25]	[26]	[29]	[33]	[36]	[37]	This work
Horizontal	0.9719	0.0020		0.0004	0.0020	0.0019	0.0057	0.0036	0.0062	0.0020
Vertical	0.9850	−0.0009	−0.0876	0.0021	−0.0007	0.0038	0.0024	0.0023	0.0052	−0.0018
Diagonal	0.9639	0.0016	0.0056	−0.0038	−0.0014	−0.0019	0.0027	0.0039	0.0069	−0.0015

Information Entropy comparison $c = 1$										
			Ciphered Image							
Test Image	Size	Original Image	[22]	[25]	[26]	[29]	[35]	[37]	[38]	This work
Lena	256 × 256	7.5690				7.9970				7.9993
Lena	512 ×512	7.4455	7.9952	7.9874	7.9970		7.9994	7.9962	7.9992	7.9993
Baboon	256 ×256	6.6962				7.9974				7.9990
Baboon	512 ×512	7.3582		7.9860	7.9969		7.9993	7.9971	7.9991	7.9993
Barbara	512 ×512	7.6321		7.9867						7.9993
Camman	256 ×256	6.9046		7.9780	7.9972	7.9967		7.9969		7.9993

Referring to Table 2, measuring the MI of ciphered images for different keys, the highest and least sensitivities are very close, thus the opponent cannot distinguish which parameter is being varied in the key. Comparing the average performance of the presented work of values around 0.1340, which is less than the average performance obtained by others [27,28].

In Table 6, the entropy of the proposed system is being compared with the results obtained in some references, with the case of positive bifurcation with the generalized parameter $c = 1$, showing that the results of this work prove the system to have very good performance. All the images used for comparison are of extension '. bmp'.

A comparison of the proposed cryptosystem with respect to the correlation coefficients of ciphered image Lena.bmp, with different previous works, is also presented in Table 6, highlighting the efficiency of the system.

Conclusions

The generalization of the Double-Humped logistic map was presented in this paper. The GDH map was used for pseudo-random number key generation (PRNG) in a medical image encryption system. The general parameter added more control on the chaotic range of the map. Changing the general parameter resulted in a new special map with a zooming effect of the bifurcation diagram. The dynamic behavior of the generalized map is analyzed, including the study of the fixed points and stability ranges and the complete bifurcation diagram. The option of designing any specific map is made possible through changing the general parameter increasing the randomness and controllability of the map. An image encryption algorithm is introduced based on pseudo-random sequence generation using the proposed generalized DH map offering secure communication transfer of medical MRI and X-ray images. Different tests are applied to the proposed encryption system, including sensitivity test, histogram analysis, correlation coefficients, MAE, NPCR and UACI calculations ensuring the effectiveness of the system. NIST analysis was performed to prove the system efficiency. Comparison was performed relative to other systems presented in literature validating the proposed system efficiency.

Conflict of interest

The authors have declared no conflict of interest.

Compliance with Ethics Requirements

This article does not contain any studies with human or animal subjects.

References

[1] Ausloos M, Dirickx M. The logistic map and the route to chaos from the beginnings to modern applications. Springer; 2006.
[2] Strogatz SH. Nonlinear dynamics and chaos: with applications to physics, biology, chemistry, and engineering. Addison-Wesley; 1994.
[3] Pellicer-Lostao C, López-Ruiz R. A chaotic gas-like model for trading markets. J Comput Sci 2010;1:24–32.
[4] Malek K, Gobal F. Application of chaotic logistic map for the interpretation of anion-insertion in poly-ortho-aminophenol films. Synth Met 2000;113(1–2):167–71.
[5] Bodnar M, Forys U. Three types of simple DDE's describing tumour growth. J Biol Syst 2007;15(4):1–19.
[6] Singh N, Sinha A. Chaos-based secure communication system using logistic map. Opt Lasers Eng 2010;48(3):398–404.
[7] Radwan AG, AbdElHaleem SH, Abd-El-Hafiz SK. Symmetric encryption algorithms using chaotic and non-chaotic generators: a review. J Adv Res (JAR) 2016;7(2):193–208.
[8] Patidar V, Sud KK, Pareek NK. A pseudo random bit generator based on chaotic logistic map and its statistical testing. Informatica 2009;33:441–52.
[9] Zidan MA, Radwan AG, Salama KN. Random number generation based on digital differential chaos. In: IEEE 54th international midwest symposium on circuits and systems (MWSCAS); 2011.p. 1–4.
[10] Coiteux K. An introductory look at deterministic chaos. Mathematics Undergraduate Thesis, Paper 2; 2014.
[11] Radwan AG. On some generalized logistic maps with arbitrary power. J Adv Res (JAR) 2013;4:163–71.
[12] Ismail SM, Said LA, Rezk AA, Radwan AG, Madian AH, Abu-Elyazeed MF, et al. Generalized fractional logistic map encryption system based on FPGA. AEU Int J Electron Commun 2017;80:114–26.
[13] Ismail SM, Said LA, Rezk AA, Radwan AG, Madian AH, Abu-ElYazeed MF, et al. Image encryption based on double-humped and delayed logistic maps for biomedical applications. In: 6th International conference in modern circuits and systems technologies (MOCAST), IEEE; 2017. p. 1–4.
[14] Pacurar EE, Sethi SK, Habib C, Laze MO, Martis-Laze R, Haacke EM. Database integration of protocol-specific neurological imaging datasets. NeuroImage 2016;124:1220–4.
[15] Wituła R, Słota D. Cardano's formula, square roots, Chebyshev polynomials and radicals. J Math Anal Appl 2010;363(2):639–47.
[16] Olivares EI, Vazquez-Medina R, Cruz-Irisson M, Del-Rio-Correa JL. Numerical calculation of the Lyapunov exponent for the logistic map. In: IEEE 12th international conference on mathematical methods in electromagnetic theory; 2008. p. 409–11.
[17] Pisarchik AN, Flores-Carmona NJ, Carpio-Valadez M. Encryption and decryption of images with chaotic map lattices. Chaos 2006;16(3):033118.
[18] Pisarchik AN, Zanin M. Image encryption with chaotically coupled chaotic maps. Physica D 2008;237(20):2638–48.
[19] Soma S, Sen S. A non-adaptive partial encryption of grayscale images based on chaos. Proc Technol 2013;10:663–71.
[20] Telem ANK, Segning CM, Kenne G, Fotsin HB. A simple and robust gray image encryption scheme using chaotic logistic map and artificial neural network. Adv Multimedia 2014;19.
[21] Zhu ZL, Zhang W, Wong KW, Yu H. A chaos-based symmetric image encryption scheme using a bit-level permutation. Inf Sci 2011;181(6):1171–86.
[22] Pareek NK, Patidar V, Sud KK. Diffusion–substitution based gray image encryption scheme. Digital Signal Process 2013;23(3):894–901.
[23] Abd-El-Hafiz SK, Radwan AG, Abd El-Haleem SH. Encryption applications of a generalized chaotic map. Appl Math Inf Sci 2015;9(6):3215.
[24] Wang XY, Yang L, Liu R, Kadir A. A chaotic image encryption algorithm based on perceptron model. Nonlinear Dyn 2010;62(3):615–21.
[25] Liu H, Wang X. Image encryption using DNA complementary rule and chaotic maps. Appl Soft Comput 2012;12(5):1457–66.
[26] Wang XY, Zhang YQ, Bao XM. A novel chaotic image encryption scheme using DNA sequence operations. Opt Lasers Eng 2015;31(73):53–61.
[27] Zhang YQ, Wang XY. A symmetric image encryption algorithm based on mixed linear–nonlinear coupled map lattice. Inf Sci 2014;20(273):329–51.
[28] Zhang YQ, Wang XY. A new image encryption algorithm based on non-adjacent coupled map lattices. Appl Soft Comput 2015;31(26):10–20.
[29] Wang X, Liu L, Zhang Y. A novel chaotic block image encryption algorithm based on dynamic random growth technique. Opt Lasers Eng 2015;31(66):10–8.
[30] Liu H, Wang X. Color image encryption based on one-time keys and robust chaotic maps. Comput Math Appl 2010;59(10):3320–7.
[31] Liu H, Wang X. Color image encryption using spatial bit-level permutation and high-dimension chaotic system. Opt Commun 2011;284(16):3895–903.
[32] Alvarez G, Li S. Some basic cryptographic requirements for chaos-based cryptosystems. Int J Bifurcation Chaos 2006;16(08):2129–51.
[33] Zhang Q, Wang Q, Wei X. A novel image encryption scheme based on DNA coding and multi-chaotic maps. Adv Sci Lett 2010;3(4):447–51.
[34] Wang X, Teng L, Qin X. A novel colour image encryption algorithm based on chaos. Signal Process 2012;92(4):1101–8.
[35] Telem AN, Segning CM, Kenne G, Fotsin HB. A simple and robust gray image encryption scheme using chaotic logistic map and artificial neural network. Adv Multimedia 2014;2014:19.
[36] Zhang Q, Guo L, Wei X. Image encryption using DNA addition combining with chaotic maps. Math Comput Modell 2010;52(11):2028–35.
[37] Wei X, Guo L, Zhang Q, Zhang J, Lian S. A novel color image encryption algorithm based on DNA sequence operation and hyper-chaotic system. J Syst Softw 2012;85(2):290–9.
[38] Fouda JA, Effa JY, Sabat SL, Ali M. A fast chaotic block cipher for image encryption. Commun Nonlinear Sci Numer Simul 2014;19(3):578–88.
[39] Dong CE. Color image encryption using one-time keys and coupled chaotic systems. Signal Process Image Commun 2014;29(5):628–40.
[40] Wu Y, Noonan JP, Agaian S. NPCR and UACI randomness tests for image encryption. J Sel Areas Telecommun 2011:31–8.
[41] Rukhin A, Soto J, Nechvatal J, Smid M, Barker E. A statistical test suite for random and pseudorandom number generators for cryptographic applications. Booz-Allen and Hamilton Inc Mclean Va; 2001.