

Chaotic Encryption Algorithm Based on Gingerbreadman Map with Adaptive Symmetry

Petr Fedoseev¹, Dmitry Pesterev², Vladislav Rozhkov³, Vyacheslav Rybin⁴ and Denis Butusov⁵

*Youth Research Institute, St. Petersburg Electrotechnical University "LETI", 5, Professora Popova st., 197376 Saint Petersburg, Russia, ^αComputer-Aided Design Department, St. Petersburg Electrotechnical University "LETI", 5, Professora Popova st., 197376 Saint Petersburg, Russia.

ABSTRACT The security of sensitive data is a crucial issue in the information age. While the existing encryption protocols cannot always guarantee the required level of security due to the rapidly increasing computational capability of attackers, developing new cryptographically strong encryption techniques is of great importance in modern computer science. One of the advanced approaches in the field of cryptography is chaos-based encryption. In this study, we propose an efficient algorithm for arbitrary multimedia data encryption using the novel finite-difference scheme with adaptive symmetry based on the Gingerbreadman chaotic map. In the experimental part of the study, we use several analysis techniques to prove the presence of chaos in the dynamics of the reported discrete map and investigate the dependence between system dynamics and symmetry coefficient. Parametric chaotic sets and the largest Lyapunov exponent plots are given to evaluate the dynamics of the investigated finite-difference model. NIST statistical tests were applied to assess the properties of the developed pseudo-random numbers generator, and correlation analysis was performed to evaluate the secrecy of the encrypted image. It is experimentally shown, that varying the symmetry coefficient can significantly increase the keyspace for the encryption algorithm based on the symmetric Gingerbreadman map. The results of this study can be used to develop encryption software, including secure text messengers or stream data ciphers.

KEYWORDS

Discrete chaos
Gingerbreadman map
Pseudo-random number generation
Chaos-based encryption
Symmetric map

INTRODUCTION

Pseudo-random number generators are broadly used in cryptography (Menezes *et al.* 2018) and mathematical simulations when implementing or imitating various stochastic processes (Rubinstein and Kroese 2016). One of the basic pseudo-random number generators is a linear congruential generator based on linear equations with modulo operation. The progress of nonlinear science and algorithms has brought multiple applications of deterministic chaos into the field. It is known, that chaotic properties like exponential divergence of trajectories or topological mixing have a strong correlation with the requirements that are typical to cryptographic systems (Qayyum *et al.* 2020).

In the last decades, there have been numerous attempts to develop text, sound, image, and stream encryption schemes based on

chaos. The key component of such chaos-based encryption algorithms is the pseudo-random generator, which provides necessary diffusion and confusion properties. One of the crucial elements of a digital pseudo-random number generator is the bit extraction method. There are several known approaches to bit extraction: the comparison of values produced by the chaotic map with a certain constant which is often calculated as a mean value or mixing with values produced by another map with the same distribution (Elmanfaloty and Abou-Bakr 2019; Irfan *et al.* 2020), extraction of several least significant bits from floating or fixed point precision number (Tutueva *et al.* 2020; Hobincu and Datcu 2018). In addition, there are even more complicated schemes that combine the previously mentioned methods with various discrete operations like modulo (Wang and Cheng 2019; El-Latif *et al.* 2022; Liu *et al.* 2017; Moysis *et al.* 2020). To resolve the relevant problem of chaos degradation in low-bit hardware, advanced techniques for increasing the length of the oscillation period were developed, e.g. perturbation of chaotic sequences (Garcia-Bosque *et al.* 2018).

The core of a discrete chaos-based pseudo-random number generator is usually a chaotic map (or mapping) in the form of the finite-difference equation. Many implementations of encryption schemes based on chaotic maps are known from literature (Elkamchouchi *et al.* 2020; Maolood *et al.* 2022; Sethi *et al.* 2022;

Manuscript received: 13 June 2024,

Revised: 25 October 2024,

Accepted: 19 December 2024.

¹psfedoseev@etu.ru

²dopesterev@etu.ru

³vrozhkov@stud.etu.ru

⁴vgrybin@etu.ru

⁵dnbutusov@etu.ru (Corresponding author)

Kanso *et al.* 2022; Alghamdi *et al.* 2022). There are two key methods commonly used in image encryption algorithms - confusion and diffusion. Confusion involves changing the pixel positions, while diffusion alters the color values of the pixels. One of the well-known confusion methods is Arnold's confusion method. For instance, in (Liu *et al.* 2016), the Arnold transform is combined with the hyperchaotic map to encrypt the image by confusion. Another approach, described in (Zhang and Wang 2014), involves performing the Arnold transformation on pixel blocks and then using a composite key as the initial value for a chaotic sequence to scramble the image. In addition, some cyclic shift methods have been proposed recently, such as the one introduced in (Wang and Gao 2020), which employs a chaotic shift transform to alter pixel positions and uses row and column replacement for pixel confusion. Some researchers go even further and try to incorporate various field-specific techniques such as DNA coding with both hyperchaos and one-dimensional composite chaos in order to obtain highly stable and robust encryption algorithms (Wan *et al.* 2020).

Further development of chaos theory led to more sophisticated image encryption algorithms. For example, DNA encoding has been combined with chaos theory to enhance image encryption methods in (Wang *et al.* 2022; Wen and Lin 2024; Liang and Zhu 2023). In (Wang and Su 2021), a new key is generated using the original image and a public key. The rows and columns of the image are then scrambled using a PWLCM generation matrix, and the resulting image is encrypted using DNA encoding. The study (ul Haq and Shah 2021) introduces a diffusion mechanism called DMRNRP, which is based on random numbers related to the plain text. The DNA sequence is diffused using this mechanism, and then converted to decimal format according to DNA decoding rules, resulting in three equal images. In (Talhaoui and Wang 2021), a pseudo-random sequence generated by CML (coupled map lattice) is used to perform bit-wise XOR operation on the pixels of the plain image.

The resulting image is then subjected to DNA encoding to obtain a DNA matrix, which is used to generate new initial conditions for CML. Additionally, in (Liu and Wang 2011), an image encryption scheme based on a four-wing hyperchaotic system, compressed sensing, and DNA encoding is proposed. Finally, in (Abuturab 2020), an image encryption algorithm that combines a quantum chaotic map, Lorenz chaotic map, and DNA coding is designed, improving both the reliability and security of the encryption scheme. In this paper, we consider the possibility of constructing a reliable chaos-based pseudo-random number generator with an increased key space from a well-known and relatively simple Gingerbreadman chaotic map. One technique for encrypting the message using the Gingerbreadman chaotic map and S_8 permutations was previously described in (Khan and Asghar 2018). However, the Gingerbreadman map in its original form does not provide a sufficient key space and the choice of encryption key is complicated due to its relatively limited dynamics.

In our study, we used an adaptive symmetry approach to construct the improved symmetric version of the Gingerbreadman map and investigate its superior properties using the analysis methods of nonlinear dynamics and mathematical statistics. The main contributions of the presented research are as follows:

1. A novel 2D symmetric chaotic map based on a modified Gingerbreadman map is introduced;
2. The pseudo-random generator with extended key space is developed using an adaptive symmetry approach;

3. The statistical and nonlinear analysis shows the applicability of the proposed solution to the encryption tasks.
4. The encryption algorithm based on the symmetric Gingerbreadman map is presented and verified experimentally.

The rest of the paper is organized as follows. Section 2 describes the proposed modification of a Gingerbreadman chaotic map and provides phase space and LLE analysis. In Section 3 we present and evaluate the pseudo-random generation algorithm based on the proposed chaotic map using the NIST tests. Section 4 is devoted to the encryption algorithm based on the proposed chaotic map. Correlation and histogram analysis are applied to analyze the security of image encryption with the proposed technique. Finally, section 5 concludes the paper.

SYMMETRIC GINGERBREADMAN MAP

The Gingerbreadman map is a well-known chaotic mapping (Barnsley *et al.* 1988). Such maps as logistic map, or the Arnold's Cat map (Xiao *et al.* 2009) can be used in cryptography to construct ciphertext sequences. However, there are some known issues with chaos-based encryption, namely, the chaos degradation in finite precision hardware implementations and limited key space of computationally simple chaotic maps. Let us construct a novel discrete dynamical system with symmetric properties using the approach described in (Karimov *et al.* 2017; Butusov *et al.* 2018).

$$\begin{aligned} x_{n+1} &= -y_n + s(b|x_n| + a) \\ y_{n+1} &= x_n - (1-s)(b|x_{n+1}| + a) \end{aligned} \quad (1)$$

where $s = 0.5$, $a = 1$, $b = 1$ are parameters of the map.

The proposed map possesses not only geometrical symmetry of the phase space but also allows backward-in-time calculation of x_n point using x_{n+1} by swapping the operators in the right-hand side function of the map. The equation 1 is obtained as follows. The key operation is handling a delta pulse before and after the autonomous rotation achievable during a small time interval when the delta pulse takes place and the phase variables are getting incremented. The original Gingerbreadman map is a modification of a non-damped system, from which the Henon map (Henon 1976) can be derived as:

$$\begin{aligned} \dot{x} &= y \\ \dot{y} &= -x - (x^2 + a) \sum_{n=-\infty}^{\infty} \delta(t - Tn), \end{aligned} \quad (2)$$

where the absolute value of the x variable is being taken instead of a square in the right-hand side function of the y :

$$\begin{aligned} \dot{x} &= y \\ \dot{y} &= -x - (b|x| + a) \sum_{n=-\infty}^{\infty} \delta(t - Tn), \end{aligned} \quad (3)$$

Thus, following the key principles of obtaining a symmetric map (Butusov *et al.* 2018) from a non-symmetric one, the increment of phase variables occurs in a small time interval ($nT, nT + \epsilon$), when there is a delta pulse present:

$$\begin{aligned} x(t + \epsilon) &= x(t) + \epsilon y(t) \\ y(t + \epsilon) &= y(t) - \epsilon x(t) - (|x| + a) \end{aligned} \quad (4)$$

By denoting $x(t + \epsilon) = x^+, x(t) = x_0, y(t + \epsilon) = y^+, y(t) = y_0$ and taking $\epsilon \rightarrow 0$ one can obtain:

$$\begin{aligned} x^+ &= x_0 \\ y^+ &= y_0 - (|x| + a) \end{aligned} \quad (5)$$

Taking into account, that between any delta pulses the system is autonomous, one might get an exact solution on a finite time interval τ :

$$\begin{pmatrix} x(t + \tau) \\ y(t + \tau) \end{pmatrix} = \begin{pmatrix} \cos(\alpha) & \sin(\alpha) \\ -\sin(\alpha) & \cos(\alpha) \end{pmatrix} \begin{pmatrix} x(t) \\ y(t) \end{pmatrix} \quad (6)$$

Combining equations 5 and 6 and dividing a delta pulse into two parts - one applied before the autonomous rotation and one after it, one can obtain a new symmetric map:

$$\begin{pmatrix} x_{n+1} \\ y_{n+1} \end{pmatrix} = \begin{pmatrix} \cos(\alpha) & \sin(\alpha) \\ -\sin(\alpha) & \cos(\alpha) \end{pmatrix} \begin{pmatrix} x_n \\ y_n - s(b|x_n| + a) \end{pmatrix} + \begin{pmatrix} 0 \\ (1-s)(b|x_{n+1}| + a) \end{pmatrix} \quad (7)$$

Where α , is a perturbation parameter, connected to the perturbation frequency. For $\alpha = \frac{3\pi}{2}$ the following holds:

$$\begin{aligned} x_{n+1} &= -y_n + s(b|x_n| + a) \\ y_{n+1} &= x_n - (1-s)(b|x_{n+1}| + a) \end{aligned} \quad (8)$$

The proposed system possesses three parameters: s is responsible for the symmetry of the system and the corresponding affine transform of the phase space, b is a bifurcation parameter, which changes the general dynamics of the map and a is responsible for a map scale, "zooming" the phase space in and out.

By varying the b coefficient one can change the behavior of the map, either driving it into a harmonic regime of oscillations or redistributing its chaotic seas and islands of stability in chaotic mode. Considering the map as a source of pseudo-random numbers, one needs to choose this parameter value carefully because the system is required to be in a chaotic regime to keep the topological mixing on the desired level. In this paper, we will refer to the b coefficient as the 'distribution coefficient'.

As one can see from Figure 1, varying the b coefficient changes the size, position, and distribution of the stability islands in a chaotic sea. While different values of b correspond to various map dynamics, all depicted phase portraits still possess horizontal symmetry, unlike the original Gingerbreadman map. Let us vary the adaptive symmetry coefficient s in the symmetric Gingerbreadman map (1). One can see from Figure 2 that the phase portrait of the map can be stretched, compressed, and rotated by changing s while preserving the overall dynamics of the map that was initially set by the b parameter value.

Let us plot the relative density-based colored one-dimensional bifurcation diagrams (Moysis et al. 2023) to illustrate how the parameter influences the dynamics of the proposed chaotic map. In our study, we use a modified version of the density-color bifurcation analysis tool proposed in (Kopets et al. 2024). The modification consists of calculating the relative density of points for each parameter value (for each vertical line) separately. Also, histograms are calculated over the entire range of values of the state variable. This approach allows one to mark the ranges of values of the state variable with greater contrast and more clearly depict the orbits that are close to periodic. Bifurcation diagrams for the proposed map are shown in Figure 3.

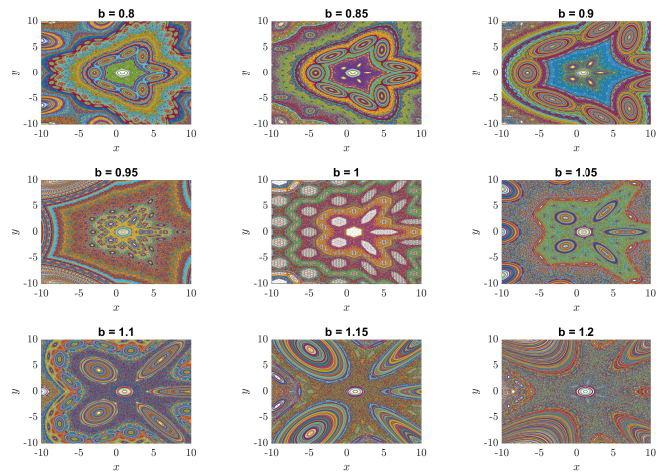


Figure 1 The phase portraits of the proposed symmetric map acquired by varying the distribution coefficient b . The value of the symmetry coefficient is fixed and equals 0.5. Different colors represent trajectories of the system's variables obtained by slightly varying the initial conditions in the range of $[-10; 10]$.

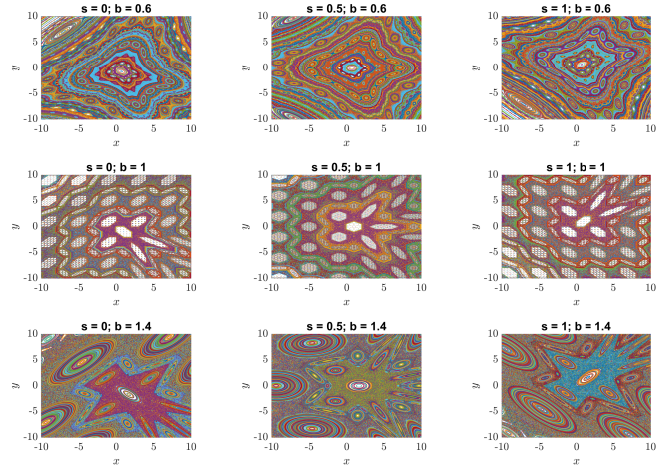


Figure 2 Phase spaces of the symmetric Gingerbreadman map plotted for various values of symmetry and distribution coefficients. One can see that for every map simulated with a symmetry coefficient $s = 0.5$, the phase space is symmetric with respect to $y = 0$ axis

Taking into account the deformation of phase space shown in Figure 2 and relative density-based colored one-dimensional bifurcation diagrams shown in Figure 3, one can hypothesize that the developed map possesses a keyspace larger than the keyspace of the original map due to the introduction of the symmetry parameter. It should be noted, that usage of chaotic maps in cryptography requires strict fulfillment of certain conditions set. A most known version of such conditions was proposed by Alvarez et al. in their comprehensive work on chaos-based cryptosystems (Alvarez and Li 2006):

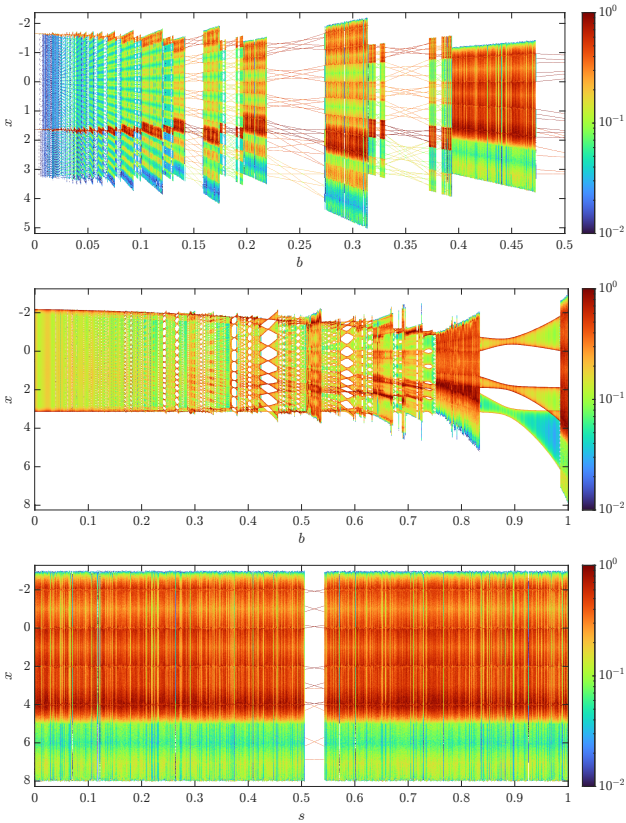


Figure 3 Relative density-based colored bifurcation diagram for the symmetric Gingerbreadman map for variable parameters a , b and s .

1. The key should be precisely defined;
2. The keyspace from which valid keys are to be chosen should be precisely specified and non-chaotic regions must be excluded;
3. The useful chaotic region should be discretized in such a way that the avalanche effect is guaranteed, i.e. two ciphertexts encrypted by two slightly different keys $k_1, k_2 \in K$ will be completely different;
4. To provide sufficient security against brute-force attacks, the key space size should be $k > 2^{100}$.
5. The ciphertext should be statistically undistinguishable from the output of a truly random function, and should be statistically the same for all keys.

In order to satisfy the requirements for keyspace size, chaotic maps with multiple bifurcation parameters and state variables are usually considered (Gafsi et al. 2020; Elgendy et al. 2016). However, implementing the map with extra parameters makes it complex to cope with the second rule. In such a case, a thorough analysis of the map properties including the Largest Lyapunov Exponent calculation and bifurcation diagrams plotting must be held. The third rule is often satisfied after the second one due to the nature of chaotic systems properties and a generally high velocity of trajectory divergence even when the difference in initial conditions or parameters of the systems is relatively small.

Evaluating the chaotic properties of symmetric Gingerbreadman map

By calculating the largest Lyapunov exponents for the system under investigation, one may evaluate the influence of s and b coefficients on the dynamics of the proposed map. In order to analyze the behavior of the map we will use two-dimensional diagrams with respect to initial conditions and different values of a distribution coefficient b and symmetry coefficient s .

Let us perform the LLE analysis of the symmetric Gingerbreadman map with the same sets of initial conditions as for experiments shown in Figure 1. One can see that the discovered islands of stability correspond directly to the empty spaces and areas with periodic trajectories on the phase portraits. Analyzing the results further, we can correctly identify the required range of parameters and initial conditions that are suitable for the generation of the desired chaotic key space.

Let us calculate the LLE values for the proposed map. The symmetric Gingerbread map 1 is a finite-difference equation of order two, thus the Jacobian matrix will have a size of 2×2 and can be written as:

$$J = \frac{dF(y_n)}{d(y_n)} = \begin{bmatrix} s \text{bsign}(x) & -1 \\ 1 - (1-s) \text{bsign}(-y + s(b|x| + a)) & s \text{bsign}(x) \end{bmatrix} \quad (9)$$

In order to obtain the largest Lyapunov exponent for a specific system with designated initial conditions set one might consider initializing a unit vector $R_0 = \text{randvec}, \|R_0\| = 1, i = 1, 2, \dots, N$, where N is the number of iterations of the finite-difference scheme, in the way that:

$$R_i = J R_{i-1} \quad (10)$$

where R'_i is the result of vector normalization $\frac{R_i}{\|R_i\|} = R'_i$ on every iteration of the finite-difference scheme. After the calculation of the desired number of iterations k has been finished, one can combine all expansions $\|R_i\|, i = 1, 2, \dots, N$ in the following way:

$$\frac{1}{N} \sum_{i=1}^N \ln \|R_i\| = L, \quad (11)$$

where L is the largest Lyapunov exponent value which can be used to detect the general presence of chaos and quantify the stability of the map.

If the LLE value for certain parameters and initial conditions is not positive, then the map is not chaotic and the trajectories starting in close proximity will not diverge. The results of LLE analysis for various initial conditions and parameter values are presented in Figures 4 and 6.

By varying the symmetry coefficient s one can transform the phase space of the map, rotating it clockwise by choosing values that are less than 0.5 and counter-clockwise by doing the opposite (Figure 5). The resulting maps preserve chaotic properties, but the distribution of chaotic oceans and islands of stability in the phase space changes (Figure 6)

Figure 6 shows that the largest Lyapunov exponents are positive for almost the whole considered space initial conditions. However, the stability islands are being stretched and rotated following the deformation of the state space, so the initial conditions are to be chosen with care.

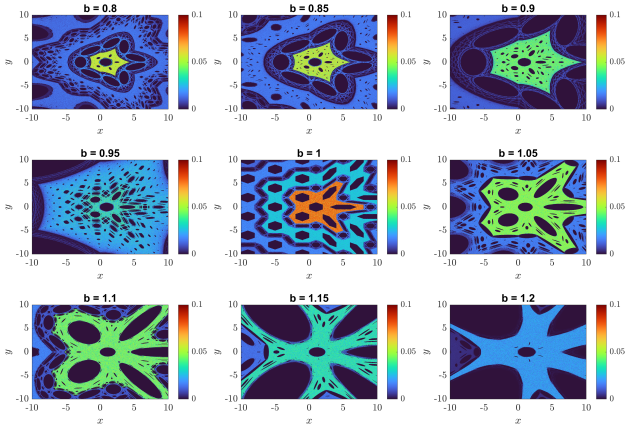


Figure 4 Two-dimensional LLE diagrams for the proposed adaptive symmetric Gingerbreadman map. Dark blue regions represent the islands of stability, where the map possesses non-chaotic behavior, and all the other colors correspond to the chaotic oceans, where the map trajectory highly depends on the chosen initial conditions.

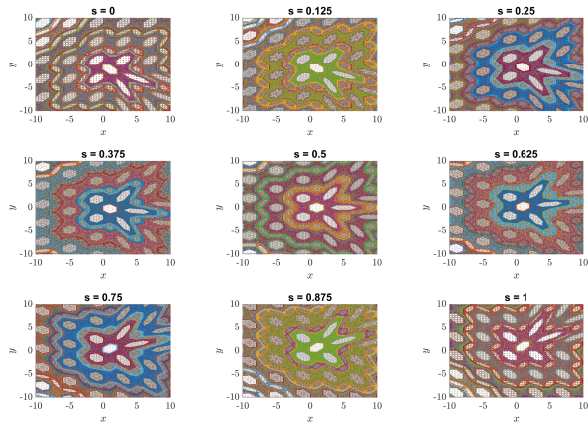


Figure 5 Phase space diagrams of symmetric Gingerbreadman map obtained by varying the symmetry coefficient s . The general symmetry of the phase space is preserved.

CONSTRUCTING A PSEUDO-RANDOM NUMBERS GENERATOR

The main idea of using the adaptive symmetric chaotic map as the pseudo-random number generator is that the bifurcation properties of such maps are not significantly affected by the changes in the symmetry coefficient. Besides, using additional coefficients allows one to increase the keyspace of the pseudo-random generator thus improving the cryptographic strength of the corresponding encryption algorithm. Taking into account a specific range of parameters where the trajectories of the map remain consistently chaotic it is possible to obtain the keyspace which is limited only by chosen data type restrictions. If the initial values for the system produce trajectories that remain inside the chaotic sea together with manipulations over the symmetry and distribution coefficients, the resulting cyphertexts are going to be completely different even if the distance between two chosen parameter values is very small.

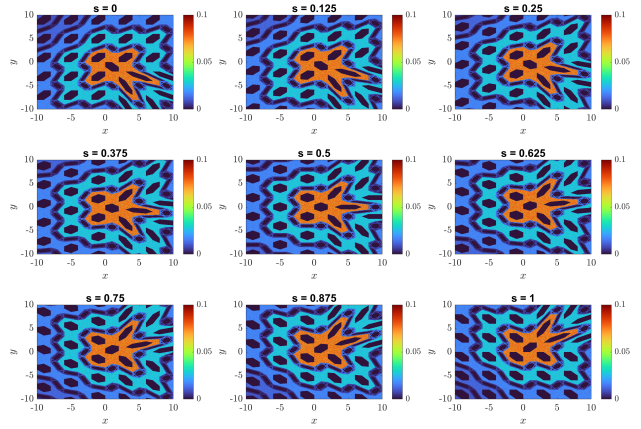


Figure 6 LLE map obtained using various values of symmetry coefficient s . All experiments were held for different initial conditions in the interval $[-10; 10]$ for both x and y with a resolution of 10,000 points per axis.

The dimension of the proposed symmetric map equals two (x_0 and y_0), and there are 3 key parameters (a , b , s) that control the behavior of the map, giving 5 potential keys total. To apply the developed map to encryption purposes one needs to evaluate the possible range of parameters at which the map exhibits chaotic behavior. This range can not be easily specified because the map behavior may change significantly based on each set of parameters. For every chosen parameter set it is required to confirm if this set is suitable for generating the chaotic sequence. Let us investigate the behavior of the system with parameter values chosen from the range of $[0; 1]$, allowing us to use any of the 2^{53} variations for a single parameter.

The initial conditions, on the other hand, can be taken almost arbitrarily, which float64 data type provides (2^{64} possible values). The comparative analysis of LLE (Figure 6) and phase space (Figure 5) diagrams shows that the choice of initial conditions is more predictable, and we will take them from the range of $[-10; 10]$. The exact number of suitable parameter sets for the float64 data type with 53 bits of significant precision can not be specified due to the number of experiments it would take (2^{53} per single parameter, making it 2^{159} possible combinations of parameter values). However, we managed to conduct 2^{27} experiments in batches of 2^{19} various sets of parameters per single computing iteration. Then a percentage of appropriate sets where the map possesses chaotic behavior was taken for every batch and the average value for the whole set of 2^{27} experiments was found. Initial conditions were chosen randomly in the range of $[-10; 10]$ for each experiment. The parameter values were chosen over the whole possible plane in the specified parameter range of $[0; 1]$ with a resolution of 1024 for both a and b coefficients and with a resolution of 512 for a symmetry coefficient s . 10,000 map iterations per set were performed.

The acquired results have shown that the amount of possible parameter sets over the specified plane is around 62%. We then took the approximate value and expanded it over the whole set making it $(2^{159}) \times 53\% \times 2^{128}$ which equals 2^{286} possible key sets that drive the map into a chaotic regime. Thus, the proposed map fulfills the abovementioned requirement for the keyspace size of the chaotic system used as the foundation of cryptographic algorithms (Smart et al. 2018; Li et al. 2018; Hu et al. 2017). The comparative table of keyspace sizes for some chaos-based encryption algorithms is presented in Table 1.

Table 1 Comparative table of key space sizes for some chaos-based encryption algorithms

Algorithm	Keyspace Size
Proposed scheme	2^{265}
Based on Chen's chaotic map (Guan et al. 2005)	2×10^{42}
Based on DNA sequences and chaotic maps (Liao et al. 2018)	2^{194}
Based on chaos in spatially extended systems (Song et al. 2013)	2^{216}

The generation of the ciphertext and the whole process of encoding in this paper follows the approach similar to the Vernam cipher (Foster 1997):

1. Generate a sequence of $(x_k, y_k), k = 1, 2, \dots, M$ values using the proposed symmetric map and the provided key. $M = n * 12$, where n is the length of a sequence required to be sent;
2. In order to get a cipher sequence one should convert obtained values of $x_k, k = 1, 2, \dots, M$ into their binary representation and pick 52 bits from every value. Thus, the sequence of ones and zeros with a random distribution is obtained. The randomness can be proven by using the NIST test suit, which is performed further in this study;
3. The ASCII code of every symbol in a message is divided into three parts corresponding to hundreds, tens, and ones;
4. Every part of the symbol is converted from decimal to binary, thus requiring $3 * 4 = 12$ bits per symbol;
5. A bit-wise operation over both sequences using the exclusive OR (XOR) operator is performed. As a result, one gets a sequence of data encrypted with a chosen cipher key.

To clarify the encryption algorithm further, we provide a block diagram presented in Figure 7.

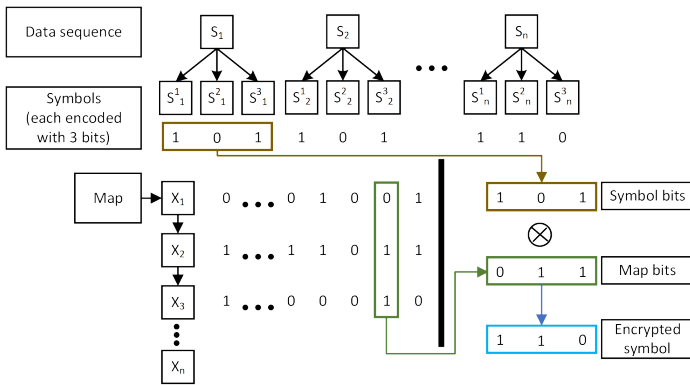


Figure 7 Block diagram of the Vernam Cipher algorithm for text data encryption coupled with proposed ciphertext generation scheme.

To decipher the encrypted information one can use the reversed algorithm, taking the ciphered sequence and using XoR with the cipher key to obtain the original data sequence.

In order to evaluate the randomness of the developed pseudo-random numbers generator based on the symmetric Gingerbreadman map we applied NIST statistical tests with various combinations of keys. Experiments were held for multiple sequences obtained from the proposed finite-difference scheme (see Figure 8). The parameters for the map were taken from the chaotic sea areas using the abovementioned LLE diagrams and were as follows: $x_0 = 1.3, y_0 = 0.1, s = 0.13, a = 1, b = 1$.

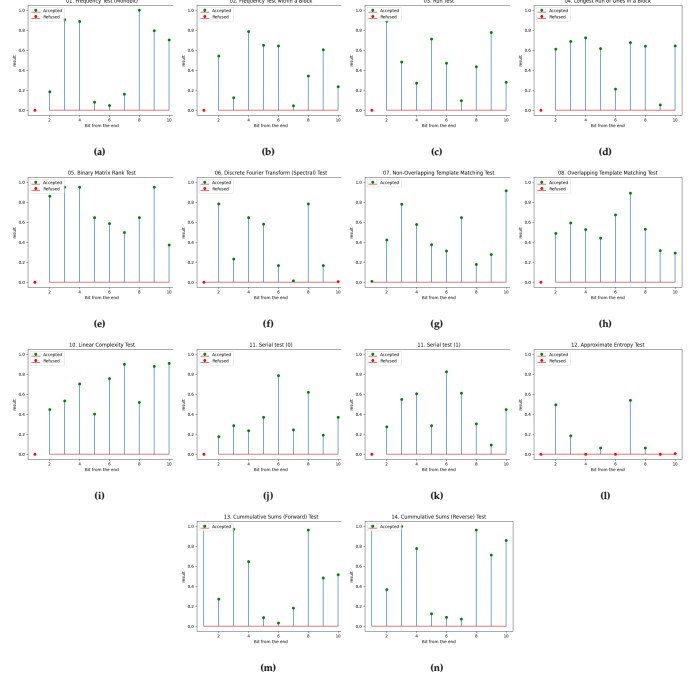


Figure 8 Results of NIST tests (a – n) held over the cipher key sequences made from the bits taken from the end of the binary representation of x values generated using symmetric Gingerbreadman chaotic map.

The results of the NIST tests show that obtaining a cipher sequence that is indistinguishable from a truly random one can be achieved using any of the bits from the end of the binary system representation. However, to quantify the impact of a symmetry coefficient on the statistical properties of the generated sequences, we performed additional tests with symmetry value variation. In the next group of tests, we analyzed the influence of symmetry coefficients chosen from the range $[0.02; 1]$ on system dynamics. The rest of the parameters are as follows: $a = 1, b = 1, (x_0, y_0) = (3.15; 0.1)$.

By performing NIST tests over the sequences acquired from the pseudo-random number generator based on the symmetric Gingerbreadman map we discovered that the obtained sequence is indistinguishable from a truly random one and thus the fifth requirement for chaos-based cryptosystems (5) is satisfied. Besides, the value of the symmetry coefficient must be chosen with care and might provide different effects for various parameters' values, but it certainly allows one to considerably increase the keyspace without significant overhead computational costs.

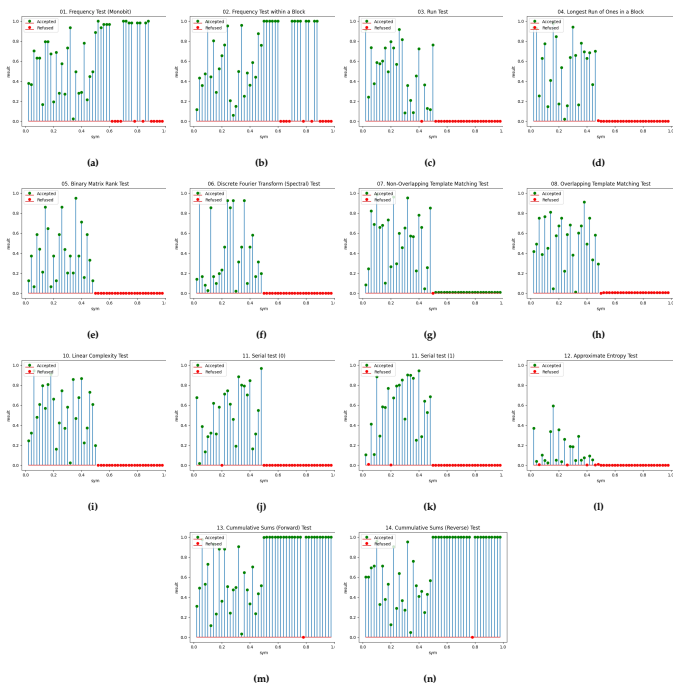


Figure 9 Results of the NIST tests for a cipher key sequence generated by taking the 5th bit from the end of a binary representation of each x value from 1,000,000 iterations of symmetric chaotic map.

ENCRYPTION ALGORITHM BASED ON THE KEY SEQUENCE OBTAINED FROM THE SYMMETRIC GINGER-BREADMAN MAP

Using the proposed pseudo-random number generator one can obtain a bit sequence to be a cipher key allowing one to encrypt and decrypt certain information. We need to specify some key points in order to perform the quality analysis of the proposed scheme as follows:

1. Statistical properties of the encrypted data should not be distinguishable from such a digital noise source
2. The decryption process must correctly reconstruct the original information even if the noise is present in the transmission channel

In the case of an encryption algorithm being applied to an image with an RGB color scheme, the basic algorithm requires some modifications. The data stream is to be represented as a sequence of red, green, and blue values in the range of $[0; 255]$ grouped as 3 per pixel. Each color value is coded by 8 bits, where the highest value of 255 would be represented in a binary form as "1111111", thus requiring a ciphertext sequence with the length of $8 \times 3 = 24$ to encrypt each pixel value. In the case of the encryption algorithm based on the chaotic pseudo-random number generation, it requires 24 iterations of the chaotic map from the chosen starting point. For a picture with the resolution of 256×256 pixels, it will require a total of $256 \times 256 \times 3 \times 8 = 1572864$ iterations, but in our case we double this amount to perform an additional encryption cycle, providing both *vertical* and *horizontal* encryption of the data, thus making the end total $1572864 \times 2 = 3145728$. The schematic representation of the proposed encryption

algorithm with a picture with the resolution of 3×3 is given in Figure 10.

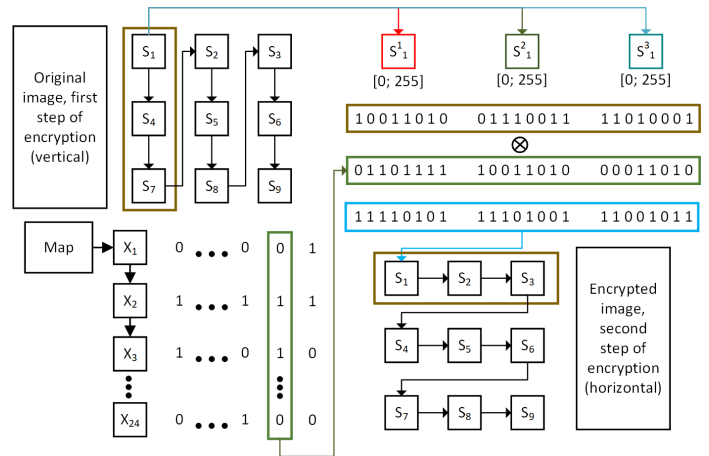


Figure 10 Schematic representation of the encryption process applied to the picture with the size of 3×3 pixels.

In order to evaluate the statistical properties of the cryptographic algorithm and the encrypted images we analyzed the histograms of color distribution (Figure 11) and performed a correlation analysis (Figure 12) over a classic sample image named *Baboon.png*. The more balanced the distribution of the histogram is, the better the encryption algorithm copes with its task (Ahmad and Hwang 2016).

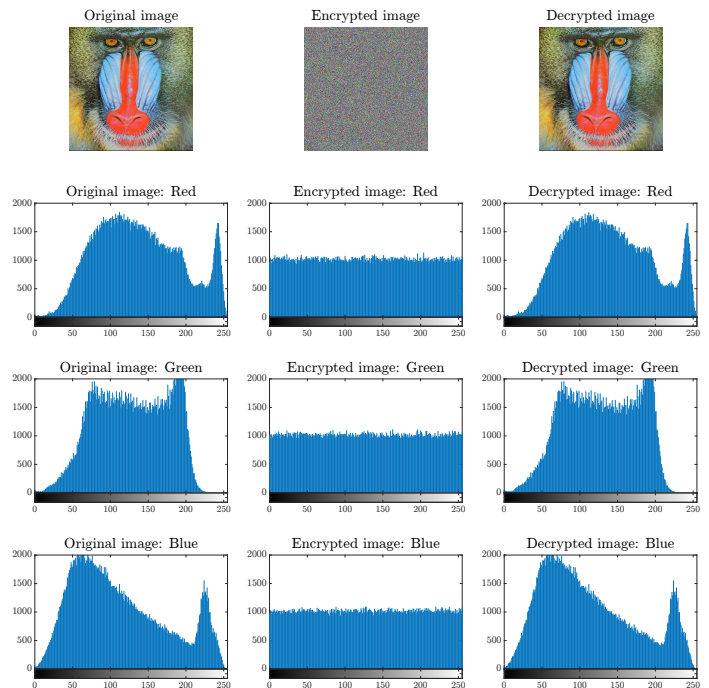


Figure 11 Original, encrypted and decrypted images of *Baboon.png* and the histogram analysis for each RGB channel.

The obtained results show that the histogram analysis of an encrypted image cannot reveal the image from digital noise, thus fulfilling the first condition for encryption algorithms. In comparison with other discussed chaotic encryption algorithms (Liao et al. 2018; Song et al. 2013) one might see that the histogram distribution

is fairly uniform, but the decryption result is significantly more accurate to the original image in terms of color representation.

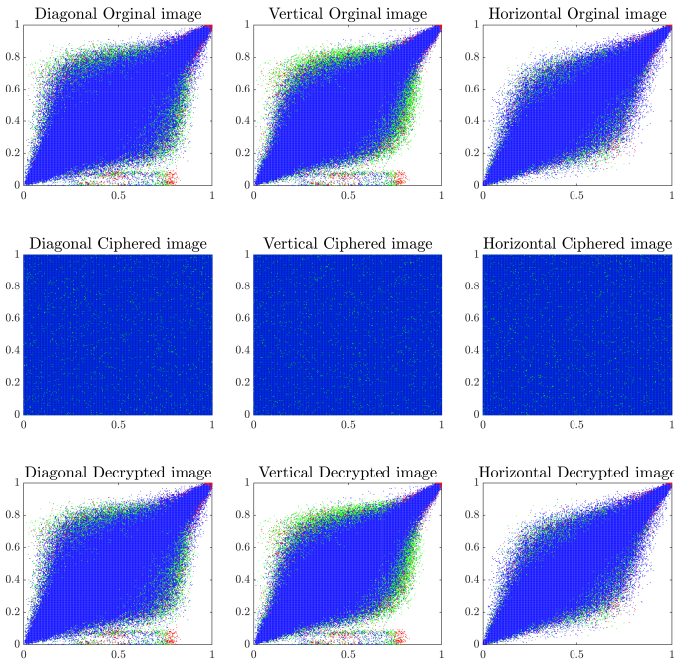


Figure 12 Correlation coefficient analysis for original, cyphered and decrypted *Baboon.png*.

By observing the correlation diagrams for a pair of adjacent RGB pixels, one can come to the conclusion that the considered encryption algorithm perfectly copes with its task. The correlation is even over the whole image plane and leaves no traces that could reveal the image from noise source data. The absolute values of correlation coefficients for each of the color channels are close to 0, while for the original image, they are close to 1. It shows that the correlation of the original data is almost non-existent (Table 2).

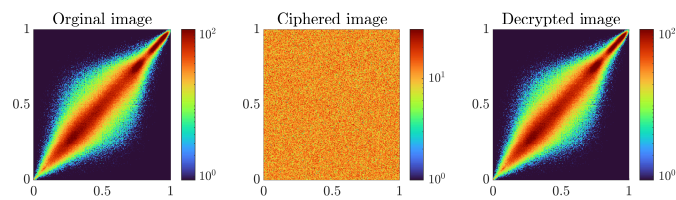


Figure 13 Density for diagonal direction correlation coefficient analysis.

The density distribution of correlation coefficients is also even over the image plane and the values of the correlation coefficients are minuscule for each of the three color channels (Table 2).

The resulting correlation copes with state-of-the-art methods proposed by other scholars in the field (Wan et al. 2020; Alghamdi et al. 2022). The general encryption algorithm based on an adaptive symmetric Gingerbreadman map is less complex than the ones proposed by the mentioned authors, being significantly less demanding in terms of computational efficiency while still providing satisfactory encryption results.

Table 2 Correlation coefficient of pair adjacent RGB pixels for *Baboon.png*.

Original Image			
	Diagonal	Vertical	Horizontal
Color	0.8097	0.8373	0.8986
Cyphered Image			
	Diagonal	Vertical	Horizontal
Color	0.0023	0.0012	0.0013
Cyphered Image (Wan et al. 2020)			
	Diagonal	Vertical	Horizontal
Color	-0.0021	-0.0001	0.0006
Cyphered Image (Alghamdi et al. 2022)			
	Diagonal	Vertical	Horizontal
Color	0.0068	0.0074	-0.0142

In order to evaluate the efficiency of the proposed technique we performed several experiments with different types of digital noise being applied to the encrypted data before decrypting it to the original state. These experiments allowed us to evaluate the noise sustainability of the algorithm. We used the Gaussian noise of different intensities, replicating the data loss that may appear in the physical data transmission channel. The sustainability is evaluated based on the analysis of the peak signal-to-noise ratio (12), which uses the mean square error between parts of the data (in our case the values of pixel colors).




$$PSNR = 10 \log_{10} \left(\frac{peakval^2}{MSE} \right), \quad (12)$$

$$MSE = - \frac{1}{n * m} \sum_{i=1}^n \sum_{j=1}^m (A(i,j) - B(i,j))^2, \quad (13)$$

where $peakval = 255$ is a peak signal level for uint8 data type, which is being used in our case to store original and deciphered images, $A(i,j)$ and $B(i,j)$ are the pixel values from the color channel for original and deciphered images respectively.

One can see, that after the application of Gaussian noise, the picture is still visually recognizable after the decryption. Thus it can be concluded that the proposed algorithm allows recovering the original information even after the transferred data has been corrupted by a significant amount of digital noise. Performing the comparison with the state-of-the-art encryption algorithms performance analysis proposed by authors in (Kanso et al. 2022) and (Pourasad et al. 2021) one may find that even with higher intensity of applied Gaussian noise, the proposed algorithm shows high sustainability to noise attacks. The most interesting comparison can be done with (Kanso et al. 2022), where Gaussian noise application of rather low intensity corrupts the final result by a significant amount.

■ **Table 3** PSNR values obtained for images with different intensities of Gaussian noise applied to an encrypted *Baboon.png*.

Noise Intensity	PSNR Value (dB)	Decrypted Image
0.02	14.7647	
0.05	14.4312	
0.1	13.4722	

Informational entropy can be analyzed by taking each of the color channels of an image and processing it by using the following formula:

$$-\sum_{i=0}^{n-1} p_i \log_2 p_i, \quad (14)$$

where n is the number of gray levels (for a single color channel) and p_i is the probability of a pixel having gray level i .

If the entropy value comes close to 8, it means that the image is uniform and the amount of information is close to none, thus making it indistinguishable from a noise source (Table 4).

■ **Table 4** Information entropy for an original and encrypted image obtained with the proposed algorithm

Image	Entropy value
Original image	7.6444
Encrypted image	7.9764

The information entropy analysis shows that the technique proposed by authors in (Liao *et al.* 2018; Song *et al.* 2013) provides a slightly more uniform distribution of pixels across the image plane with an increase of roughly 1.2% between experiments on different test pictures. The resulting encrypted image is still can be considered indistinguishable from the digital noise source, but the results may differ depending to the encryption key parameters.

When one uses a chaotic map to generate a cipher text, the plaintext attack can be resisted, because there is no correlation between information entropy and adjacent pixels for both all-black and all-white test images (Figure 14, Table 5), and the patterns in the resulting encrypted image are mainly determined by the chaotic sequence.

The results of statistical properties evaluation show that the proposed encryption technique provides a simple approach to increasing the available key space size without any significant computational overheads compared to the conventional chaos-based encryption algorithms.

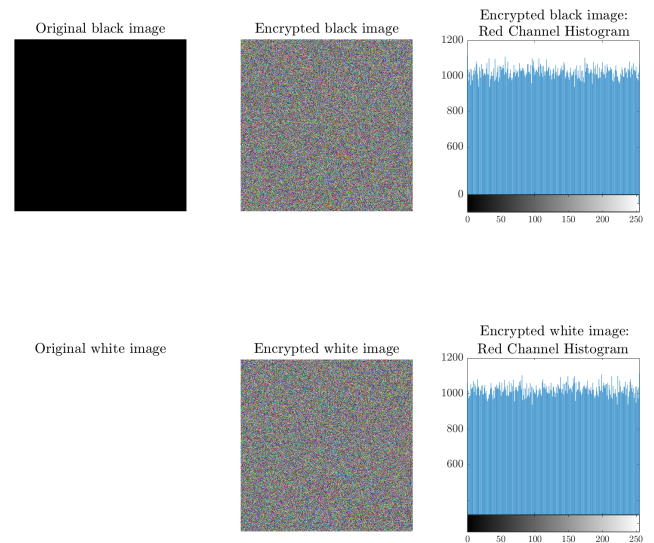


Figure 14 Red channel histograms of encrypted data for black and white images representing a chosen plaintext attack.

■ **Table 5** Information entropy for encrypted data obtained from pure white and black images as a result of chosen plaintext attack.

Picture	Information Entropy
Black Original	0
Black Ciphered	7.9993
White Original	0
White Ciphered	7.9993

CONCLUSION

In this study, the symmetric modification of the Gingerbreadman map was proposed. We performed phase-space, bifurcation, largest Lyapunov exponent, and statistical analysis over the proposed map to confirm its properties. Then we constructed and evaluated the corresponding pseudo-random number generator to confirm its suitability for encryption tasks. The experimental results of the chaotic properties evaluation of the proposed symmetric map proved that introducing a symmetry coefficient allows one to enrich the map's dynamics thus significantly increasing the key space of the corresponding pseudo-random number generator and resulting encryption algorithm. This statement was confirmed in this study by applying the NIST statistical tests. The histogram and correlation coefficient analysis were applied to verify the security of the proposed encryption scheme. The peak signal-to-noise ratio calculation and entropy analysis were applied to evaluate the resistivity of the proposed algorithm to noise. It should be noted, that finite-difference schemes with adaptive symmetry are implied to be more secure from the attacks based on the recognition and spectral analysis of the carrier signal (Ostrovskii *et al.* 2022; Rybin *et al.* 2022, 2023a,b), which makes a chaotic communication system based on such maps a promising direction for further research.

Acknowledgments

This study was supported by the Russian Science Foundation (RSF), project 23-79-10151.

Availability of data and material

Not applicable.

Conflicts of interest

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

Ethical standard

The authors have no relevant financial or non-financial interests to disclose.

LITERATURE CITED

- Abuturab, M. R., 2020 A superposition based multiple-image encryption using fresnel-domain high dimension chaotic phase encoding. *Optics and Lasers in Engineering* **129**: 106038.
- Ahmad, J. and S. O. Hwang, 2016 A secure image encryption scheme based on chaotic maps and affine transformation. *Multimedia Tools and Applications* **75**: 13951–13976.
- Alghamdi, Y., A. Munir, and J. Ahmad, 2022 A lightweight image encryption algorithm based on chaotic map and random substitution. *Entropy* **24**: 1344.
- Alvarez, G. and S. Li, 2006 Some basic cryptographic requirements for chaos-based cryptosystems. *International journal of bifurcation and chaos* **16**: 2129–2151.
- Barnsley, M. F., R. L. Devaney, B. B. Mandelbrot, H.-O. Peitgen, D. Saupe, *et al.*, 1988 Fractal patterns arising in chaotic dynamical systems. *The science of fractal images* pp. 137–168.
- Butusov, D. N., A. I. Karimov, N. S. Pyko, S. A. Pyko, and M. I. Bogachev, 2018 Discrete chaotic maps obtained by symmetric integration. *Physica A: Statistical Mechanics and its Applications* **509**: 955–970.
- El-Latif, A. A. A., J. Ramadoss, B. Abd-El-Atty, H. S. Khalifa, and F. Nazarimehr, 2022 A novel chaos-based cryptography algorithm and its performance analysis. *Mathematics* **10**: 2434.
- Elgendy, F., A. M. Sarhan, T. E. Eltobely, S. F. El-Zoghdy, H. S. El-Sayed, *et al.*, 2016 Chaos-based model for encryption and decryption of digital images. *Multimedia tools and applications* **75**: 11529–11553.
- Elkamchouchi, H., W. M. Salama, and Y. Abouelseoud, 2020 New video encryption schemes based on chaotic maps. *IET Image Processing* **14**: 397–406.
- Elmanfaloty, R. A. and E. Abou-Bakr, 2019 Random property enhancement of a 1d chaotic prng with finite precision implementation. *Chaos, Solitons & Fractals* **118**: 134–144.
- Foster, C. C., 1997 Drawbacks of the one-time pad. *Cryptologia* **21**: 350–352.
- Gafsi, M., N. Abbassi, M. A. Hajjaji, J. Malek, and A. Mtibaa, 2020 Improved chaos-based cryptosystem for medical image encryption and decryption. *Scientific Programming* **2020**: 1–22.
- Garcia-Bosque, M., A. Pérez-Resca, C. Sánchez-Azqueta, C. Aldea, and S. Celma, 2018 Chaos-based bitwise dynamical pseudorandom number generator on fpga. *IEEE Transactions on Instrumentation and Measurement* **68**: 291–293.
- Guan, Z.-H., F. Huang, and W. Guan, 2005 Chaos-based image encryption algorithm. *Physics letters A* **346**: 153–157.
- Henon, M., 1976 A two-dimensional mapping with a strange attractor. *Communications in Mathematical Physics* **50**: 376–392.
- Hobincu, R. and O. Datcu, 2018 A novel chaos based prng targeting secret communication. In *2018 International Conference on Communications (COMM)*, pp. 459–462, IEEE.
- Hu, T., Y. Liu, L.-H. Gong, and C.-J. Ouyang, 2017 An image encryption scheme combining chaos with cycle operation for dna sequences. *Nonlinear Dynamics* **87**: 51–66.
- Irfan, M., A. Ali, M. A. Khan, M. Ehatisham-ul Haq, S. N. Mehmood Shah, *et al.*, 2020 Pseudorandom number generator (prng) design using hyper-chaotic modified robust logistic map (hc-mrlm). *Electronics* **9**: 104.
- Kanso, A., M. Ghebleh, and M. Bou Khuzam, 2022 A probabilistic chaotic image encryption scheme. *Mathematics* **10**: 1910.
- Karimov, A. I., D. N. Butusov, V. G. Rybin, and T. I. Karimov, 2017 The study of the modified chirikov map. In *2017 XX IEEE International Conference on Soft Computing and Measurements (SCM)*, pp. 341–344, IEEE.
- Khan, M. and Z. Asghar, 2018 A novel construction of substitution box for image encryption applications with gingerbreadman chaotic map and s 8 permutation. *Neural computing and applications* **29**: 993–999.
- Kopets, E., V. Rybin, O. Vasilchenko, D. Butusov, P. Fedoseev, *et al.*, 2024 Fractal tent map with application to surrogate testing. *Fractal and Fractional* **8**: 344.
- Li, C., D. Lin, B. Feng, J. Lü, and F. Hao, 2018 Cryptanalysis of a chaotic image encryption algorithm based on information entropy. *Ieee Access* **6**: 75834–75842.
- Liang, Q. and C. Zhu, 2023 A new one-dimensional chaotic map for image encryption scheme based on random dna coding. *Optics & Laser Technology* **160**: 109033.
- Liao, X., M. A. Hahsmi, R. Haider, *et al.*, 2018 An efficient mixed inter-intra pixels substitution at 2bits-level for image encryption technique using dna and chaos. *Optik-International Journal for Light and Electron Optics* **153**: 117–134.
- Liu, H. and X. Wang, 2011 Color image encryption using spatial bit-level permutation and high-dimension chaotic system. *Optics Communications* **284**: 3895–3903.
- Liu, W., K. Sun, and C. Zhu, 2016 A fast image encryption algorithm based on chaotic map. *Optics and Lasers in Engineering* **84**: 26–36.
- Liu, Y., Y. Luo, S. Song, L. Cao, J. Liu, *et al.*, 2017 Counteracting dynamical degradation of digital chaotic chebyshev map via perturbation. *International Journal of Bifurcation and Chaos* **27**: 1750033.
- Maolood, A. T., E. K. Gbashi, and E. S. Mahmood, 2022 Novel lightweight video encryption method based on chacha20 stream cipher and hybrid chaotic map. *International Journal of Electrical & Computer Engineering* (2088-8708) **12**.
- Menezes, A. J., P. C. Van Oorschot, and S. A. Vanstone, 2018 *Handbook of applied cryptography*. CRC press.
- Moysis, L., M. Lawnik, and C. Volos, 2023 Density-colored bifurcation diagrams—a complementary tool for chaotic map analysis. *International Journal of Bifurcation and Chaos* **33**: 2330036.
- Moysis, L., E. Petavratzis, C. Volos, H. Nistazakis, and I. Stouboulos, 2020 A chaotic path planning generator based on logistic map and modulo tactics. *Robotics and Autonomous Systems* **124**: 103377.
- Ostrovskii, V. Y., V. G. Rybin, A. I. Karimov, and D. N. Butusov, 2022 Inducing multistability in discrete chaotic systems using numerical integration with variable symmetry. *Chaos, Solitons & Fractals* **165**: 112794.
- Pourasad, Y., R. Ranjbarzadeh, and A. Mardani, 2021 A new algorithm for digital image encryption based on chaos theory.

- Entropy **23**: 341.
- Qayyum, A., J. Ahmad, W. Boulila, S. Rubaiee, F. Masood, *et al.*, 2020 Chaos-based confusion and diffusion of image pixels using dynamic substitution. *IEEE Access* **8**: 140876–140895.
- Rubinstein, R. Y. and D. P. Kroese, 2016 *Simulation and the Monte Carlo method*. John Wiley & Sons.
- Rybin, V., T. Karimov, O. Bayazitov, D. Kvitko, I. Babkin, *et al.*, 2023a Prototyping the symmetry-based chaotic communication system using microcontroller unit. *Applied Sciences* **13**: 936.
- Rybin, V., G. Kolev, E. Kopets, A. Dautov, A. Karimov, *et al.*, 2022 Optimal synchronization parameters for variable symmetry discrete models of chaotic systems. In *2022 11th Mediterranean Conference on Embedded Computing (MECO)*, pp. 1–5, IEEE.
- Rybin, V., D. Kvitko, T. Karimov, L. Nardo, E. Nepomuceno, *et al.*, 2023b Estimating optimal synchronization parameters for coherent chaotic communication systems in noisy conditions. *Chaos Theory and Applications* pp. 141–152.
- Sethi, J., J. Bhaumik, and A. S. Chowdhury, 2022 Chaos-based uncompressed frame level video encryption. In *Proceedings of the Seventh International Conference on Mathematics and Computing: ICMC 2021*, pp. 201–217, Springer.
- Smart, N., M. Abdalla, E. Bjørstad, C. Cid, B. Gierlichs, *et al.*, 2018 Algorithms, key size and protocols report (2018). ECRYPT—CSA, H2020-ICT-2014—Project **645421**.
- Song, C.-Y., Y.-L. Qiao, and X.-Z. Zhang, 2013 An image encryption scheme based on new spatiotemporal chaos. *Optik-International Journal for Light and Electron Optics* **124**: 3329–3334.
- Talhaoui, M. Z. and X. Wang, 2021 A new fractional one dimensional chaotic map and its application in high-speed image encryption. *Information Sciences* **550**: 13–26.
- Tutueva, A. V., A. I. Karimov, L. Moysis, C. Volos, and D. N. Butusov, 2020 Construction of one-way hash functions with increased key space using adaptive chaotic maps. *Chaos, Solitons & Fractals* **141**: 110344.
- ul Haq, T. and T. Shah, 2021 4d mixed chaotic system and its application to rgb image encryption using substitution-diffusion. *Journal of Information Security and Applications* **61**: 102931.
- Wan, Y., S. Gu, and B. Du, 2020 A new image encryption algorithm based on composite chaos and hyperchaos combined with dna coding. *Entropy* **22**: 171.
- Wang, L. and H. Cheng, 2019 Pseudo-random number generator based on logistic chaotic system. *Entropy* **21**: 960.
- Wang, S., Q. Peng, and B. Du, 2022 Chaotic color image encryption based on 4d chaotic maps and dna sequence. *Optics & Laser Technology* **148**: 107753.
- Wang, X. and S. Gao, 2020 Image encryption algorithm for synchronously updating boolean networks based on matrix semi-tensor product theory. *Information sciences* **507**: 16–36.
- Wang, X. and Y. Su, 2021 Image encryption based on compressed sensing and dna encoding. *Signal Processing: Image Communication* **95**: 116246.
- Wen, H. and Y. Lin, 2024 Cryptanalysis of an image encryption algorithm using quantum chaotic map and dna coding. *Expert Systems with Applications* **237**: 121514.
- Xiao, D., X. Liao, and P. Wei, 2009 Analysis and improvement of a chaos-based image encryption algorithm. *Chaos, Solitons & Fractals* **40**: 2191–2199.
- Zhang, Y.-Q. and X.-Y. Wang, 2014 A symmetric image encryption algorithm based on mixed linear–nonlinear coupled map lattice. *Information Sciences* **273**: 329–351.

How to cite this article: Fedoseev, P., Pesterev, D., Rozhkov, V., Rybin, V., and Butusov, D. Chaotic Encryption Algorithm Based on Gingerbreadman Map with Adaptive Symmetry. *Chaos Theory and Applications*, 7(1), 31–41, 2025.

Licensing Policy: The published articles in CHTA are licensed under a [Creative Commons Attribution-NonCommercial 4.0 International License](https://creativecommons.org/licenses/by-nc/4.0/).

