Journal homepage: https://itce.vn.ua/en

Information Technologies and Computer Engineering **Vol. 22, No. 3. 2025**

Article's History: Received: 11.09.2025 Revised: 20.11.2025 Accepted: 23.12.2025

UDC 004.03 DOI: 10.31649/vitce/3.2025.89

Application of chaos theory to improve resilience of encryption systems in information technology

Volodymyr Lukhanin*

PhD in Physical and Mathematical Sciences, Assistant
Kharkiv National University of Radio Electronics
61166, 14 Nauky Ave., Kharkiv, Ukraine
https://orcid.org/0000-0003-4328-929X

Abstract. The study aimed to provide a theoretical justification for the use of chaotic dynamical systems to enhance the strength of cryptographic keys. The research methodology was based on theoretical, comparative and critical analysis of scientific sources to assess the potential of chaotic systems. The study determined that chaotic maps provide high entropy, long periods and unpredictability of the generated sequences due to their sensitivity to initial conditions, which is confirmed by the Shannon entropy calculations and positive Lyapunov exponents. The use of hash functions and mechanisms for updating the internal state eliminated statistical correlations and increased the resistance of generators to cryptanalysis. The study demonstrated that the sequences obtained on the basis of the logistic mapping and the Lorentz system pass the standard statistical tests of NIST SP 800-22, demonstrating uniformity of distribution and absence of correlations. The use of the Chua circle as an analogue circuit provides physically implemented True Random Number Generators with low power consumption, suitable for resource-limited Internet of Things systems. The scheme with the integration of several chaotic maps has proven to increase the key space and increase the resistance to statistical attacks compared to traditional PseudoRandom Number Generators. The study determined that chaotic generators are able to provide forward and backward secrecy by updating the internal state of the system, which prevents the sequences from repeating. Chaotic generators have advantages over traditional PseudoRandom Number Generators due to their very long periods and sensitivity to initial conditions, but their effectiveness depends on cryptographic post-processing and the correct choice of parameters. The study recommended the use chaotic systems as an additional source of entropy in software and hardware implementations, in particular, in lightweight cryptographic solutions for the Internet of Things, sensor networks and mobile devices. The practical significance is determined by the application of the results by developers for secure encryption, researchers for random number generation, and Internet of Things engineers for device security

Keywords: nonlinear dynamics; random number generators; cryptographic entropy; chaotic attractors; initialisation vectors; topological transitivity; cryptographic extraction

Introduction

Ensuring the resilience of cryptographic systems is one of the key challenges of information security in the 21st century. The growth in data transmission, the proliferation of cloud services and the rapid development of the Internet of Things (IoT) create new risks to the confidentiality and integrity of information. Traditional encryption methods, including symmetric and asymmetric algorithms, have proven to be effective, but their sustainability is gradually being questioned due to the increase in computing power and the emergence of quantum technologies (Fernández-Caramès & Fraga-Lamas, 2020). This creates a need to find new approaches to cryptographic key generation that would provide a significant level of unpredictability and security. One of these promising areas is the use of chaotic dynamical systems capable of generating sequences with high entropy and complex structure.

The scientific discourse further addresses the use of chaos in cryptography. M. Ali *et al.* (2025) proposed an approach to building an encryption system using geometric permutations and dynamic substitutions. The authors showed that the combination of chaotic maps with new methods of data structuring can significantly increase the

Suggested Citation:
Lukhanin, V. (2025). Application of chaos theory to improve resilience of encryption systems in information technology. *Information Technologies and Computer Engineering*, 22(3), 89-100. doi: 10.31649/vitce/3.2025.89

*Corresponding author

cipher's resistance to linear and differential analysis. This forms a new combination strategy that improves the resistance of classical chaotic algorithms. The practical application of chaotic models in resource-constrained environments was demonstrated by T.A. Dhopavkar *et al.* (2022). The study used Tinkerbell and Duffing maps to create a data protection scheme for IoT systems. The results proved that chaotic maps can provide both lightweight algorithms and a high level of security even in devices with limited computing capabilities. This proved the suitability of chaotic maps for IoT applications with low resource requirements.

A. Belazi *et al.* (2022) addressed the protection of medical images, where data quality and reliability are critical. The study improved on the sinus tangent map and demonstrated that it produces uniform and statistically stable sequences that guarantee high ciphertext entropy. This meant that chaos proved to be an effective tool in medical cryptography. In the field of satellite imagery, promising results were shown by A. Kumar & M. Dua (2021). The study proposed to use the cosine transform in combination with chaotic maps, which improved the quality of key generation and provided an additional level of data protection. This proved the versatility of chaos as a tool for cryptographic applications in various industries.

The tendency to combine different chaotic models was reflected by M. Kumar & D. Ch (2025). The study demonstrated that merging chaotic maps with multilevel mixing techniques makes it possible to achieve system robustness to statistical analysis. In particular, multi-level shuffling significantly complicates the ability to predict keys, making brute-force attacks almost impossible. This formed an approach to integrating chaotic maps with multilevel transformations, which increases the cryptographic strength of systems by complicating the key structure. A similar direction was pursued in E. Faure *et al*. (2024), where authors proposed enhancements to classical chaos-based encryption schemes to improve key agreement and data security. An additional perspective was revealed by J. Jackson & R. Perumal (2025), employing fractional-order chaotic maps. The study determined that the use of more complex mathematical models can generate sequences with increased unpredictability and a higher degree of security. This extended the capabilities of traditional models and increased the level of cryptographic security.

In the Ukrainian scientific space, there is also considerable interest in the topic of cryptography and chaotic models. The study by A. Shandyba (2025) contributed to the practical application of chaos for information security, in particular in the field of digital watermarks. The study demonstrated that the use of chaotic maps when embedding markers ensures the system's resistance to attacks and preserves the authenticity of multimedia data. This confirmed the potential of chaos as a tool not only for key generation but also for expanding the range of cryptographic applications. O. Krulikovskyi *et al*. (2024) analysed the periodicity of time series generated by a logistics map, taking into account the limited accuracy of digital computing. The study highlighted that the limitations of machine arithmetic can lead to the degradation of chaos and the emergence of periodic structures, which directly affects the reliability of cryptographic generators based on chaotic models. The study revealed critical aspects of the implementation of chaotic algorithms in digital systems and emphasised the need to incorporate computational accuracy when developing chaos-based cryptographic mechanisms.

Despite the numerous results, most studies focus on applied tasks, image security, IoT, or medical data. However, there is a lack of generalised theoretical models that systematically describe how chaos can be used to generate keys in a broader cryptographic context. In addition, much of the research is focused on individual chaotic maps, which could not be used to assess the potential of a comprehensive approach to combining them. This creates a gap between the theoretical basis and practical applications. Therefore, the study aimed to theoretically study the possibilities of using chaotic dynamic systems to increase the strength of cryptographic keys. To achieve this goal, the following tasks were performed: to systematise and formalise the properties of chaotic dynamic systems that determine their suitability for cryptographic applications, to present a three-stage model of chaos-based key generation, to evaluate the efficiency, practical stability and potential of the model for use in symmetric, asymmetric and hybrid cryptosystems.

Materials and Methods

The study included a theoretical comprehensive review of chaotic dynamical systems and their models, the creation of an abstract key generation scheme, an assessment of practical applications, limitations, and a comparison with traditional generators to determine their cryptographic potential. The research included four stages. At the first stage, the method of generalising scientific approached to chaotic dynamical systems and their application in cryptography was applied in the following areas: symmetric and asymmetric algorithms, steganography and multimedia, hardware solutions (True Random Number Generator (TRNG), IoT). This systemised and assessed the level of entropy, unpredictability, and resistance to cryptanalysis. The task of this stage was to determine the potential of chaotic systems as an effective source of entropy for encryption and information security protocols.

At the second stage, the method of theoretical analysis was used to test the suitability of chaotic systems for generating random sequences in cryptography. The mathematical and physical models of chaos, such as the logistic mapping (provides a simple implementation and is used to generate pseudorandom numbers), the Lorentz system (demonstrates complex multidimensional trajectories with high unpredictability), and the Chua circle (can be used for chaos at the hardware level, making it suitable for TRNG and IoT solutions), were considered to test their suitability for generating random sequences in cryptography. The choice of these models was justified by the fact that they

represent different levels of complexity, from simple mathematical constructions to multidimensional and hardware solutions. The study analysed their properties (topological mixability, transitivity, high entropy, long periods, and practical non-repeatability) and presented a generalised abstract model of key generation, which includes quantisation of values, cryptographic extraction (SHAKE256, Hash-based Message Authentication Code (HMAC)-based Key Derivation Function (HKDF)), and internal state update (reseeding). The stage aimed to show how chaotic trajectories can be transformed into cryptographically strong key material with high entropy and unpredictability.

The third stage presented an abstract model of key generation that combines the dynamics of chaotic systems with cryptographic primitives to obtain a stable key material with high entropy, no correlations, and the ability to protect symmetric, asymmetric, and hybrid encryption systems. In addition, real-life examples of chaotic models in cryptography, such as logistic mapping, the Lorentz system, and hybrid maps, were analysed to assess their effectiveness in generating random sequences, encrypting images, and expanding the key space. The critical analysis also identified the limitations of chaos-based generators and ways to improve their reliability, which is the basis for the practical use of chaotic systems in cryptography. The task of this stage was to determine the conditions under which chaos-based generators can be used in cryptography without losing their stability, as well as to formulate practical requirements that compensate for the lack of strict mathematical guarantees of their security.

In the fourth stage, the method of comparative analysis was used to compare chaotic generators and traditional PRNGs according to key criteria – nature, entropy, periodicity, predictability, speed, implementation features and application in cryptography, which determined their advantages and limitations. These criteria were chosen because they determine the suitability of a generator for cryptography. Nature reflects the principle of operation and the source of randomness, entropy and periodicity characterise the quality of the generated sequences, predictability is directly related to attack resistance, speed and implementation determine practical efficiency, and application in cryptography shows real applicability in data protection protocols. This identified the strengths and weaknesses of both approaches: to show the advantages of chaotic systems in providing high entropy, practical unpredictability and long periods, to highlight the disadvantages and to assess their suitability for use in cryptosystems. The methods of theoretical generalisation, critical analysis and comparative review of scientific sources were used to analyse and compare the models.

Results and Discussion

Nonlinear dynamic systems and their cryptographic applications in random number generation

A nonlinear dynamical system is defined as a mathematical model of processes in which the state change depends not only on time but also on previous values, and there are nonlinear relationships between the variables. Such systems are usually described by systems of differential equations or mappings, where the output is not proportional to the input. Characteristic properties include the presence of multiple equilibrium states, the ability to transition to unstable modes, self-organisation and the formation of complex behaviour even based on simple rules. Nonlinearity is the key source of chaotic regimes, in which the system demonstrates a complex and almost unpredictable evolution (Ming *et al.*, 2023).

In the field of cryptography, a fundamental aspect is the quality of random numbers used at all stages of data protection. In "symmetric encryption algorithms" (Advanced Encryption Standard (AES), ChaCha20, Data Encryption Standard (DES)), chaotic generators can be used to generate key material. The initial conditions and parameters of chaotic maps define a wide key space, which ensures the uniqueness and cryptographic strength of the obtained values. In addition, chaos can be used to generate the initialisation vectors required in Cipher Block Chaining (CBC), Counter Mode (CTR) and Galois/Counter Mode (GCM), where the randomness of the Initialisation Vector (IV) is a critical condition for protection against repetition. As proven by M.J.A. Calderon *et al*. (2024), in stream ciphers (ChaCha20-Poly1305), the uniqueness of the nonce is crucial to prevent reuse of the key stream, and it is the sensitivity of chaotic systems to initial conditions that can achieve such uniqueness.

In "asymmetric algorithms" (Rivest-Shamir-Adleman (RSA), Elliptic Curve Cryptography (ECC), as well as post-quantum schemes Kyber, Saber) with a public key, chaos can act as an auxiliary source of randomness. In particular, random values derived from chaotic processes can be used to generate seeds and parameters in RSA or ECC-based schemes (in Optimal Asymmetric Encryption Padding (OAEP)), which eliminates the problem of determinism. Additionally, chaotic maps are suitable for generating one-time random numbers required in key exchange protocols such as Diffie-Hellman and Elliptic Curve Diffie-Hellman (ECDH), increasing the resilience of systems to prediction (Garipcan *et al.*, 2025).

Chaotic permutations and maps are used in steganography to form complex patterns of data placement in images and multimedia files. This makes it much more difficult to detect hidden messages. Additionally, chaotic processes ensure the creation of watermarks that are resistant to attacks aimed to delete or modify. At the level of hardware implementations, chaotic oscillators, in particular the Chua circle, in combination with cryptographic extractors, can function as TRNGs (Nazish *et al.*, 2025). Such solutions are particularly relevant for embedded systems, sensor networks, and IoT devices, where the combination of high entropy and low power consumption is a critical requirement.

In practice, "hybrid cryptosystems" are mostly used, where asymmetry is used to securely transmit a symmetric key, and the data is encrypted directly using a symmetric

algorithm. The security of such systems directly depends on the entropy level of the initial random numbers from which the key material is formed. A critical component of cryptographic protocols is "random number generators". Insufficient entropy of keys (less than 128 bits) makes the system vulnerable to brute-force attacks. In the opinion M.J.A. Calderon *et al.* (2024), repeated nonces or IVs create conditions for key stream replay and recovery attacks. The lack of proper randomness in authentication protocols opens the way to replay attacks, and the predictability of the "k" parameter in digital signature schemes (Elliptic Curve Digital Signature Algorithm (ECDSA), Digital Signature Algorithm (DSA)) can lead to compromise of the private key.

Random number generators form the basis of modern cryptography of the 21st century, since the quality of their work directly determines the stability of cryptographic algorithms. The use of chaotic systems as a source of randomness is appropriate and fits seamlessly into the context of symmetric and asymmetric encryption, as well as additional applications, such as steganography and hardware solutions. In chaotic dynamic systems, attractors are central – sets to which trajectories tend over time. The so-called strange attractors, which have a fractal structure and multidimensionality, are fundamental; they determine the behavioural patterns of the system, not being reduced to regular periodicity. Another fundamental feature is the sensitivity to initial conditions: even minor changes in the initial parameters lead to fundamentally different development trajectories. This phenomenon, known as the "butterfly effect", directly contributes to the unpredictability of chaotic processes (Ding *et al.*, 2024). At the same time, a chaotic system remains deterministic, but due to the exponential growth of errors due to nonlinearity, its long-term behaviour cannot be accurately predicted.

Among the most common mathematical and physical models of chaos, there are several that are studied in the context of cryptography. The logistic mapping is a classical one-dimensional model of chaotic dynamics that describes the population dynamics of a system with limited resources. It can be used to generate pseudo-random numbers due to its ability to demonstrate chaotic behaviour at certain parameter values. The mathematical expression of the logistic mapping is as follows (May, 1976):

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

where: x_n – value at the n-th step (the state of the system at time n); r – parameter that controls the dynamics of the system; x_{n+1} – value at the next step. This model can exhibit chaotic behaviour at certain values of the parameter , and its simplicity makes it common for applications such as pseudorandom number generation in cryptography.

A general discrete chaotic system is a system described by recurrent equations that reflect the relationship between the next and previous state of the system and has the form (Poincaré, 2017):

$$x_{n+1} = f(x_n, \theta), \quad (2)$$

where: θ – parameter that can be used to control a system, for example, it can affect the level of chaos or the transition between regular and chaotic behaviour; $f(x_n, \theta)$ – function that determines how a previous state of the system affects the next. Such a system is characterised by sensitivity to initial conditions, which is one of the main properties of chaos. Even a small change in the parameter θ can cause significant changes in the behaviour of the system.

The E.N. Lorenz (1963) system is a classic example of a three-dimensional nonlinear dynamical system consisting of three differential equations. It was developed for modelling atmospheric convection, but eventually became an icon of chaos theory due to its interesting and unpredictable properties, in particular, due to the E.N. Lorenz attractor, which shows how the system transitions between different states, and has the following form (3-5):

$$\dot{x} = \sigma (y - x); \quad (3)$$

$$\dot{y} = x (p - z) - y; \quad (4)$$

$$\dot{z} = xy - \beta z, \quad (5)$$

where: $\dot{x}$, $\dot{y}$, $\dot{z}$ – time derivatives that describe changes in each of the system variables; x – horizontal velocity (or convection); y – temperature or heat flux; σ – determines the rate of differentiation of the variable x relative to y, i.e. convection rate or flow rate; p – determines the temperature gradient or temperature difference between different layers of the atmosphere; β – describes vertical flows in atmospheric models or systems that demonstrate convection phenomena, z – vertical flow or vertical motion in systems. All parameters in the Lorentz system determine the interaction between temperature, convection rate and vertical flows in the medium. Changing any of these parameters can lead to a change in the behaviour of the system, from stable to chaotic. The Lorentz system is an example of a complex physical model that can be applied both at the mathematical level and in real-world cryptographic applications, such as key generation and encryption protocols.

As an electronic circuit, the Chua circle can be used to implement chaotic oscillations at the hardware level. It consists of an inductor, two capacitors, and a nonlinear resistive element (the so-called Chua diode), which can be used to exhibit a wide range of chaotic modes. The simplicity of the design and the possibility of physical implementation make this scheme a promising candidate for the creation of hardware chaotic signal generators that can be used in cryptography and information security systems (Alibraheemi *et al.*, 2024).

One of the key properties of chaotic systems is topological mixability. In phase space, this is manifested in the fact that any initial region of trajectories is eventually distributed over the entire domain of the definition. The system's trajectory visits an arbitrary neighbourhood with

a non-zero probability, which, for cryptography, means that there are no local patterns in the generated sequences, which ensures an even distribution of information and increases resistance to cryptanalysis. Another critical characteristic is high entropy and a rich state space. Entropy is a measure of disorder, which can be quantitatively described using formula (6) by C.E. Shannon (1948):

$$H(X) = -\sum_{ip}(x_i)\, log_2\, p\,(x_i), \quad (6)$$

where: $H(X)$ – entropy of a random variable X, which is a measure of disorder or the amount of information contained in a sequence of values X; $p\,(x_i)$ – probability of occurrence of the i-th element x_i in the sequence (the frequency of occurrence of a particular value in the data set); $log_2\, p\,(x_i)$ – logarithm of the probability of x_i in base 2, determines the number of bits required to encode the value x_i and expresses how much information this element contains. In chaotic systems, even short time series exhibit entropy values close to the maximum, making them similar to random sequences. This, in turn, provides a wide key space that is beyond the reach of brute force or effective cryptanalysis.

Another property is the long periods and the practical lack of repeatability. While traditional pseudo-random number generators have a finite period after which the sequence is reproduced, for multidimensional chaotic systems, this period can be so long that it is considered infinite from a practical point of view. This ensures the uniqueness of each generated sequence and makes it impossible to use repetition-based attacks. The fundamental basis for the use of chaos in cryptography is also provided by mathematical theorems confirming unpredictability, in particular, the positive value of the largest O.M. Lyapunov (1892) index:

$$\lambda = \lim_{n\to\infty}\frac{1}{n}\sum_{k=0}^{n-1} ln|f'(x_k)|, \quad (7)$$

where: λ – largest Lyapunov exponent, a numerical criterion of the system's chaotic nature; $\lim_{n\to\infty}$ – shows that the assessment is conducted for a very large number of iterations, i.e. in the long run; $\frac{1}{n}\sum_{k=0}^{n-1}$ – average of all iterations k from 0 to n-1, averages local indicators of trajectory divergence; $ln|f'(x_k)|$ – natural logarithm of the modulus of the derivative of the function of the current state , measures the local divergence of neighbouring trajectories in phase space. The combination of a virtually infinite period and a positive Lyapunov exponent ensures that chaotic systems generate unique and unpredictable sequences, making them effective for cryptographic use.

The theorem of H. Poincaré's (2017) recurrence theorem proves that any trajectory of a system sooner or later returns to an arbitrarily small neighbourhood of the initial point, but the moment of return is fundamentally unpredictable (8, 9):

$$\forall U \supseteq \{x_0\}, \exists\{t_n\}: \varphi\,(t_n, x_0) \in U; \quad (8)$$

$$\forall n \in U, t_n \to \infty, \quad (9)$$

where: U – any neighbourhood of the initial point x_0; t_n – time after which the system trajectory enters the neighbourhood of U; $\varphi(t_n, x_0)$ – function that describes the position of the system at the moment of time t_n. Poincaré's theorem describes a critical property of chaotic systems: although their behaviour at any given time is unpredictable, they demonstrate recurrence, i.e. the ability to return to a certain region of phase space, albeit after a long time. This property is essential for cryptography, as it can be used for the generation of long, unpredictable and unique sequences to be used as keys.

The property of topological transitivity is one of the main characteristics of chaotic systems, which states that trajectories in the system eventually cover the entire region of phase space. In mathematical terms, this property is noted as (Gottschalk & Hedlund, 1955):

$$\varphi\,(t, U) \cap V \neq \emptyset. \quad (10)$$

This means that regardless of where a trajectory starts in phase space, it will eventually become in some other region of space. The system can thus "distribute" its behaviour throughout the phase space, which is a key characteristic of chaos. In the context of cryptography, this means that, based on any initial condition, the generated sequences will be evenly distributed throughout the entire space of possible values, which ensures unpredictability and a high level of entropy. This increases the resistance of cryptographic systems to attacks, as it becomes almost impossible to predict the long-term behaviour of a generator based on a short sequence.

An abstract model of key generation based on chaotic systems involves three stages: quantisation of chaotic values, cryptographic extraction, and updating the internal state. At the first stage, the continuous values obtained from the chaotic system are converted into a discrete form by scaling and rounding them to integer values. Formally, this process can be expressed as (Knuth, 1969):

$$u_n = \lfloor 2^w \times h(x_n) \rfloor, \omega = 64 \text{ or } 128, \quad (11)$$

where u_n – discretised value; $h(x_n)$ – function that determines the chaotic value at the n-th step; ω – number of bits for scaling accuracy; 2^w – scaling of values using a power of two. ω can be 64 or 128, which means the number of bits used to determine the accuracy and magnitude of the scaling. The value ω determines how many bits will be used to store each generated value. In the following stages, after obtaining the discretised values, they are cryptographically extracted using hash functions such as SHA-256 or others, which obtained key material or pseudorandom sequences. This process ensures the creation of a high-calorie, attack-resistant key by eliminating statistical dependencies and levelling the bit distribution, increasing resistance to cryptanalysis (Menezes *et al.*, 2011).

The discretised values u_n are used as input to the *SHAKE256* cryptographic hash function along with service

parameters (nonce and iteration index) and appear as (SHA-3 Standard, 2015):

$$y_n = SHAKE256(u_n \| nonce \| I), \quad (12)$$

where *SHAKE*256 – cryptographic hash function that generates random bits based on input values. It has the properties of high resistance to cryptanalysis and can generate arbitrarily long output bit sequences, y_n – result of the *SHAKE256* hash function, which are uniformly distributed random bits that can be used in subsequent stages of cryptographic algorithms. This stage ensures that the distribution is levelled, statistical dependencies are eliminated, and uniform random bits are obtained.

The internal state is updated based on the previous state and new values of the results to ensure the absence of repeated sequences and increase resistance to cryptographic attacks, in particular, prediction-based attacks. At this stage, the internal state of the system S_t is changed using a hash function that includes both the previous state S_t and the new random bits y_n obtained from the previous stage (using the *SHAKE256* hash function) (Barker & Kelsey, 2015):

$$S_{t+1} = \mathrm{H}(S_t \| y_n), \quad (13)$$

$$(\theta, x) \leftarrow MapFrom(S_{t+1}), \quad (14)$$

where: S_t – current internal state of the system at the t-th step; *MapFrom* – function that generates new values of parameters and state variables based on the new value of S_{t+1}. This process ensures that key sequences are unrepeatable, as updated parameters and state variables generate new trajectories in phase space each time. As a result, even if the cryptographic key is used repeatedly, its complexity and unpredictability remain at a high level. Thus, this stage guarantees high entropy and the absence of predictable patterns in the generated sequences, which makes the keys resistant to cryptanalysis and increases the system's reliability.

The results of the study showed that chaotic maps are capable of generating sequences with high entropy and statistical randomness. This result was consistent with the work of M. Irfan & M.A. Khan (2024), where they proposed a cryptographically secure generator based on a robust chaotic tent map. The study proved that their model demonstrates positive Lyapunov performance and thus meets the criterion of sensitivity to initial conditions. Testing according to the NIST SP 800-22 and TestU01 standards confirmed the statistical randomness of the output bit sequences. This confirmed the notion that chaotic systems can provide high entropy and cryptographic strength of generators.

The results of the study showed the effectiveness of chaos in steganography and multimedia data protection. This correlates with the study by Z.B. Madouri *et al.* (2024), developing a new pseudorandom generator based on chaotic digital filters. The study employed it to build an image encryption algorithm and proved that the generated sequences have high entropy and uniform distribution. The test results confirmed the algorithm's resistance to statistical attacks, which indicates the absence of noticeable correlations in chaotic trajectories. Additionally, the suitability of this approach for practical use in multimedia applications requiring reliability and speed was emphasised.

D. Murillo-Escobar *et al.* (2024) studied two chaos-based generators implemented on microcontrollers. The study tested their performance and the statistical randomness of the generated sequences. The test results showed compliance with NIST SP 800-22 criteria, which confirms the cryptographic suitability of the proposed solutions. A significant observation was that the implementation on resource-limited devices provides high entropy while reducing power consumption. This corresponded to the energy efficiency and practicality of chaotic generators in sensor networks and IoT systems outlined in the current study, confirming the feasibility of their use in lightweight cryptography.

Y. Alloun *et al.* (2025) presented a Field-Programmable Gate Array (FPGA) implementation of a generator that combines chaotic maps with artificial neural networks. The study emphasised that the integration of different approaches improves resistance to cryptanalysis. The experimental results confirmed the uniformity of the generated sequences and their compliance with NIST requirements, which indicates their cryptographic suitability. This correlated with the results of the study, which emphasised the need for hybrid cryptosystems and hardware implementations. This alignment demonstrated the feasibility of using chaos as an additional source of entropy in combination with other cryptographic primitives and confirmed the prospects of hardware solutions based on chaotic dynamic systems in cryptography.

The results of the study showed that long periods, recurrence and unpredictability are fundamental characteristics of chaotic systems in cryptography. In this context, the study by V. Patidar & T. Singh (2025) examined these properties in detail, proposing a new approach to random number generation based on Hamiltonian conservative chaotic systems. The study used Poincaré sections to generate non-periodic sequences that exhibit an almost infinite period. Verification using NIST SP 800-22 standards confirmed the cryptographic reliability of the proposed generator. This correlated with the current research on the butterfly effect, Poincaré's theorem, and the practical non-repeatability of chaotic trajectories, and serves as further evidence of the importance of the mathematical properties of chaos for creating cryptographically strong random number generators.

Thus, due to their fundamental properties, chaotic dynamical systems can be a reliable basis for generating cryptographic randomness. Their use in symmetric, asymmetric, and hybrid algorithms ensures high entropy, unpredictability, and cryptographic strength of key sequences. Practical research confirms the effectiveness of chaotic systems in cryptographic protocols and the prospects for further development of lightweight solutions.

Principles of construction and practical analysis of chaotic models of cryptographic key generation

For clarity, it is advisable to present the operation of the proposed model in the form of a flowchart showing the main stages of the process, from the generation of chaotic sequences to the formation of a cryptographic key. Such an approach can be used to trace the relationship between the individual stages of the model and determine the logic of its functioning. The flowchart also serves as a tool for further analysis and optimisation, as it demonstrates which system components are central in ensuring cryptographic security (Fig. 1).

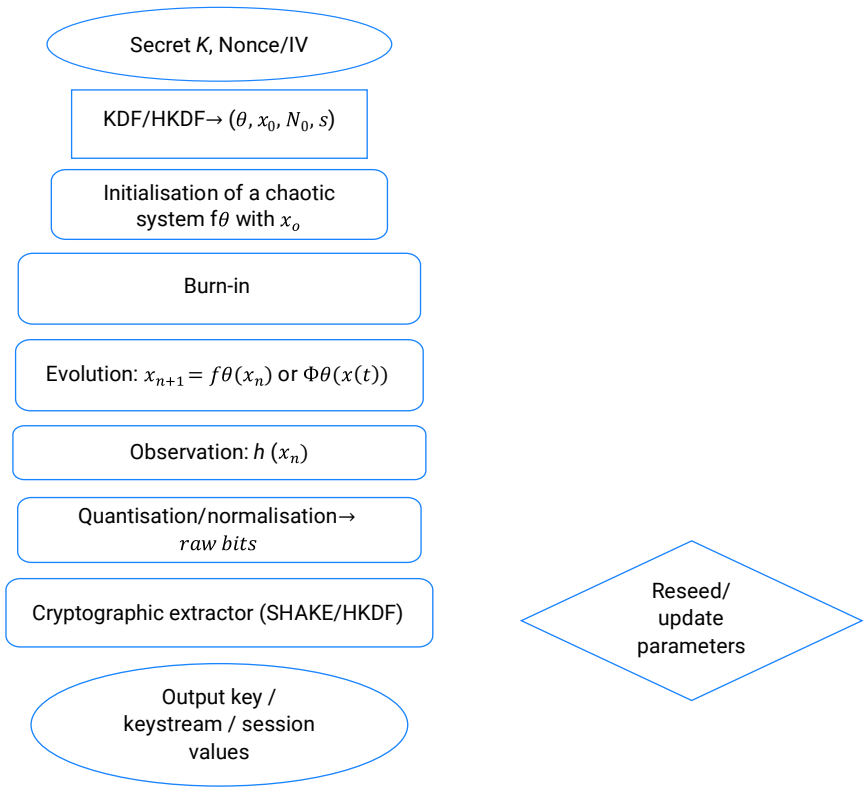

Figure 1. Flowchart of an abstract model of chaos-based key generation

Note: Secret K – secret parameters of the system that define the initial conditions of the chaotic model (Formulas 1-5); Nonce/IV – one-time random value, required for the uniqueness of the key stream (Formula 12); KDF/HKDF (θ, x_0, N_0, s) (Formulas 2, 11-14) – special function converts secret data into initial parameters of the chaotic system; Initialisation of the chaotic system f – starts the chaotic map or Lorentz system according to Formulas 1-5; Burn-in – discards initial iterations to eliminate transient effects (Formula 2); Evolution: $x_{n+1} = f\theta(x_n)$ or $\Phi\theta(x(t))$ – creation of a system trajectory based on recurrent equations (Formula 2); Obervation: $h(x_n)$ – mapping the internal state to the output data to be quantised (Formula 11); Quantisation/Normalisation (Formula 11) – continuous values into bit sequences; Cryptographic Extractor (SHAKE/HKDF, Formula 12) – levelling the distribution and removing statistical dependencies; Reseed / parameter update (Formulas 13,14) – update the internal state to ensure forward/backward secrecy; Output – key, keystream or session values for further use in cryptosystems (Formulas 12(result), 13,14)

Source: compiled by the author based on O.M. Lyapunov (1892), C.E. Shannon (1948), E.N. Lorenz (1963), D.E. Knuth (1969), A.J. Menezes *et al.* (2011), National Institute of Standards and Technology (2015), E. Barker & J. Kelsey (2015), H.M.M. Alibraheemi *et al.* (2024)

The principle of building a chaotic key model is to combine the dynamics of chaotic systems with cryptographic primitives. The initial conditions and parameters of the system are used as secret data. In the case of the logistic mapping, the key parameters are the coefficient r and the initial value x_0, while in the Lorenz system, the set of values (x_0, y_0, z_0) and the parameters σ, ρ, β. The size of the key should be sufficient to provide a space that is at least 2^{128}, as this is the minimum condition to prevent a complete search (Ming *et al.*, 2023). Next, the system evolves, resulting in a trajectory of successive states. To eliminate transient effects, burn-in is used, i.e. discarding the first iterations. The resulting values are subject to quantisation, i.e. conversion into bit sequences by scaling, mantissa extraction, or combinatorial operations (e.g. Exclusive OR (XOR)). The final step is cryptographic extraction (*SHAKE256*, HKDF), which removes patterns and ensures a uniform distribution of the output bits (Yin *et al.*, 2024).

The proposed scheme gives the model a number of properties. Firstly, the high entropy of chaotic sequences provides a level of disorder, which is quantified by the Shannon entropy. Secondly, the use of an extractor eliminates statistical correlations, making the original data appears as random data (Yin *et al.*, 2024). The sensitivity to initial conditions and parameters ensures that the same sequence cannot be reproduced without knowing the secret values, which is formally described by positive Lyapunov exponents. Updating the internal state ensures

forward and backward secrecy, and the use of hash functions with extended output makes the model scalable, capable of generating an arbitrary amount of key material with unchanged randomness characteristics (Tiwari *et al.*, 2025). Chaotic processes provide a full cycle of cryptographic key generation, from parameters and trajectories to bit sequences and their cryptographic amplification, creating a practically applicable basis for symmetric, asymmetric and hybrid encryption systems. An abstract model of chaos-based key generation combines the properties of chaotic systems with cryptographic extractors, providing a high level of entropy, uniform bit distribution, and no correlations. Updating the internal state increases resistance to compromise, while unpredictability and sensitivity to initial conditions make the model suitable for use in cryptosystems (Table 1).

Table 1. Examples of the application of chaotic generator models in cryptography

Model	Characteristic	Key objective	Results
Logistics mapping	An improved logistic map with "infinite chaos" for generating bit sequences is proposed. Implementing a logistics map as a PRNG in an FPGA	Develop a high-speed PRBG suitable for lightweight cryptography and IoT	The generator has passed NIST SP 800-22 tests; high entropy and no correlations were demonstrated. Demonstrated effectiveness for IoT and mobile devices
Lorenz system	The current cipher with a key stream generated by the Lorentz system is developed. A lightweight image encryption algorithm using Lorentz trajectories	Build a real cryptographic algorithm on a chaotic system. Ensure effective and fast image protection on mobile devices	The algorithm has shown high resistance to cryptanalysis and performance in a real-world environment. High entropy, uniformity of histograms, and resistance to statistical attacks have been achieved. Suitable for resource-limited systems
Hybrid models	Integration of Henon and Logistic maps to complicate chaotic trajectories	Improve image encryption security by expanding the key space	The algorithm has been proven to increase the key space and increase resistance to statistical and correlation attacks; it outperforms individual models

Note: PRBG – Pseudorandom Binary Generator
Source: compiled by the author based on M.J.A. Calderon *et al.* (2024), H.M.M. Alibraheemi *et al*. (2024), P.K. Singh *et al*. (2024), M. Nazish *et al*. (2025), A. Al-Hyari *et al*. (2025)

Chaotic systems have not only theoretical but also practical value in cryptography. Logistic mapping has been successfully used in both software and hardware implementations, providing high performance and entropy. The Lorentz system has been proven to be suitable for building both stream ciphers and lightweight algorithms for protecting multimedia data. The integration of several chaotic maps, as in the case of Henon and Logistic, demonstrates the possibility of further strengthening cryptographic strength by combining different models. Experimental results have confirmed the viability of chaotic generators as an alternative to classical DRBGs in various applications.

Nevertheless, it is necessary to strictly observe practical safety precautions in chaos-based generators. The use of raw chaotic trajectories without additional post-processing leads to correlations and statistical dependencies. To eliminate these problems, modern approaches use hash functions and "feedback key" mechanisms that ensure a uniform distribution of output bits and are confirmed by the results of NIST SP 800-22 tests (Yin *et al.*, 2024). In addition, the risk of "dead zones" in the parametric ranges of chaotic maps, which reduce entropy and narrow the key space, is emphasised. To solve this problem, it is proposed to use variable structures, for example, in the "structure-varying CML" model, which demonstrates a stable level of entropy and resistance to prediction (Ming *et al.*, 2023). The ultimate accuracy of calculations can cause hidden periodicity, so it is necessary to use high bit depth (64/128 bits) and regular state updates (reseeding) through cryptographic hashes. In addition, comprehensive testing is recognised as a mandatory stage of verification of chaos-based generators, which, in addition to the standard NIST SP 800-22/90B sets, includes analysis of autocorrelation functions, min-entropy estimation, and spectral methods (Ding *et al.*, 2024). Thus, scientific research has confirmed that the recommendations for the use of extractors, a wide key space, periodic state updates, and statistical testing are not only theoretically sound but also experimentally verified.

At the same time, in contrast to classical cryptographic primitives (RSA, ECC, AES-DRBG), where the security of algorithms is formally proved by reducing them to complex mathematical problems, chaos-based generators do not have security proofs. Their reliability is mostly confirmed by experimental tests (Ding *et al.*, 2024), entropy analysis (Nazish *et al.*, 2025), or numerical simulations (Calderon *et al.*, 2024), but not by formal mathematical reductions. This creates a certain gap between theory and practice, which is still under debate. Therefore, it is advisable to consider chaotic systems not as a full-fledged independent cryptographic mechanism, but as an additional source of entropy in hybrid schemes, where the final randomness is enhanced by cryptographic extractors (SHAKE, HKDF) and thus partially compensates for the lack of strict mathematical guarantees (Alibraheemi *et al.*, 2024; Singh *et al.*, 2024).

Both classical pseudorandom number generators and new approaches based on chaotic dynamical systems are used in cryptography. Classical PRNGs have advantages in terms of speed and ease of implementation, but their entropy and resistance to prediction are determined only by the quality of the algorithm. Instead, chaotic generators

use the properties of nonlinear systems, sensitivity to initial conditions, unpredictability, and almost infinite periods, which make them promising for generating cryptographic keys, nonces, and initialisation vectors (Table 2).

Table 2. Comparison of chaotic generators with traditional random number generators

Criteria	Chaotic generators	Traditional PRNG
Nature	Based on dynamic systems with nonlinear behaviour	Algorithmic designs, mainly linear or combined (linear congruent, Mersenne Twister, DRBG)
Entropy	High due to sensitivity to initial conditions and parameters, confirmed by Shannon's entropy	Depends on the algorithm; classic PRNGs have lower entropy
Frequency	Very long or almost infinite periods (in multidimensional systems)	Limited, the period depends on the bit depth
Predictability	Theoretically deterministic, but practically unpredictable due to chaos	Classic PRNGs are often predictable (if the state is known)
Performance	May be lower (mainly in differential models)	High performance, optimised for CPU/GPU
Implementation	Require precise numerical methods or hardware support (FPGA, analogue circuits)	Easy software execution
Application in cryptography	Promising for generating keys, nonces, and initialisation vectors	Standard DRBGs (AES-DRBG, Hash-DRBG, ChaCha20)

Source: compiled by the author based on H. Ming *et al.* (2023), M.J.A. Calderon *et al*. (2024), H.M.M. Alibraheemi *et al.* (2024), F. Yin *et al*. (2024), A. Tiwari *et al.* (2025), M. Nazish *et al.* (2025)

Chaotic generators demonstrate key advantages: high entropy and unpredictability due to their sensitivity to initial conditions, long periods and unique sequences, as well as the possibility of efficient software and hardware implementation. At the same time, their limitations are the loss of randomness due to finite accuracy and the lack of rigorous security proofs, which require the use of cryptographic extractors. The optimal approach is to integrate chaotic systems as an additional source of entropy in combination with classical cryptographic extractors. In practical applications, it is worth considering hardware implementations based on FPGAs and chaotic oscillators, in particular, Chua circles, which are especially relevant for IoT and sensor networks. To maintain cryptographic security, it is recommended to use regular reseeding, increased bit depth, and comprehensive statistical testing (NIST SP 800-22/90B, min-entropy analysis, spectral methods).

The results of the study showed that chaos-based generators require strict adherence to practical security considerations, as the use of raw chaotic trajectories without post-processing leads to correlations and statistical dependencies that need to be eliminated using hash functions, feedback key mechanisms, and comprehensive testing. This is consistent with the study by A. Sambas *et al.* (2024) on a dynamic analysis of a new three-dimensional chaotic system, which showed that only after careful optimisation of parameters and verification with statistical tests, PRNG demonstrates the required level of cryptographic reliability. The study emphasised the importance of spectral properties and recurrence to avoid hidden correlations. This means that the reliability of chaos-based generators can only be achieved by combining mathematical modelling, post-processing, and comprehensive testing.

Y. Alghamdi *et al.* (2022) proposed a lightweight image encryption algorithm based on a chaotic map and random substitution. The study emphasised that their approach is specifically designed for resource-constrained environments, such as mobile devices and IoT systems, where high performance and minimal power consumption are required. Experimental testing has shown that the generated sequences have high entropy, uniform histograms, and no statistical correlations. Additionally, it was proven that the algorithm demonstrates resistance to cryptanalytical attacks, including statistical and differential attacks. This correlated with the current study, which used logistic maps and the Lorenz system to build lightweight algorithms for encrypting multimedia data. This confirmed the practical feasibility of chaotic models in cryptography and proved their effectiveness in protecting information in real-world conditions.

The results of the study showed that chaotic oscillators are fundamentally different from traditional PRNGs, as they provide high entropy, long periods, and practical unpredictability, although they require complex numerical methods or hardware support for implementation. This correlates with the study by Y. Luo *et al.* (2024), who presented an FPGA implementation of a high-speed oscillator based on an n-dimensional chaotic system. The study proved that such a hardware implementation combine the characteristic properties of chaos with high performance and uniformity of output sequences. The tests have confirmed the cryptographic suitability of the generator, which proved the practical feasibility of using chaotic PRNGs in real security protocols.

The results of the study confirmed that the construction of a chaotic key generation model requires combining the dynamics of nonlinear systems with cryptographic primitives, including quantisation, extraction, and internal state updating, which ensures uniform bit distribution and forward/backward secrecy. This correlates with the study by M.A. Hadjadj *et al.* (2025), proposing a hardware implementation of PRNG-CS for embedded security systems. The authors emphasised the need to integrate chaotic dynamic processes with cryptographic post-processors to eliminate statistical correlations and increase cryptographic strength. Testing following NIST standards demonstrated

the high entropy and performance of the generator even in resource-limited environments and showed that chaotic models can be effectively implemented at the hardware level, ensuring reliable generation of key material.

M.T. Gençoğlu *et al.* (2025) presented a chaotic random number generator based on the quantum wave equation. The study emphasised that the use of chaotic dynamic properties alone is not sufficient to ensure cryptographic reliability. Therefore, they combined chaotic processes with post-processing mechanisms that eliminate correlations and guarantee a uniform distribution of the output bits. Testing has confirmed that this approach meets modern cryptographic requirements. This correlates with the results of the current study, where the integration of chaos with cryptographic extractors was recommended as the optimal solution. This proved the feasibility of combining nonlinear dynamics and classical cryptographic methods to create secure key generators.

Thus, chaos should be considered not as a self-sufficient crypto-primitive with formal security proofs, but as an additional entropy in standardised key generation circuits. This bridges the gap between chaos theory and cryptography practice and outlines a route to implementing chaos-based generators in real-world encryption, signature, and steganography protocols. In the future, this may contribute to the creation of more resilient and energy-efficient cryptographic systems.

Conclusions

The results of the study have shown that chaotic dynamical systems demonstrate a number of properties that make them promising in cryptography. The key characteristics include the presence of strange attractors with a fractal structure, sensitivity to initial conditions, and the butterfly effect, which cause unpredictability and high variability of the output sequences. Positive Lyapunov indices confirmed the exponential dependence of the trajectories on the initial parameters, which ensures that they cannot be reproduced exactly without knowing the secret values. Topological mixability and transitivity prove that chaotic trajectories are distributed uniformly in the phase space, which minimises local patterns and increases resistance to cryptanalysis. The presented model of key generation, which includes the stages of quantisation, hash extraction and internal state update, has confirmed the ability to eliminate statistical correlations and guarantee forward and backward secrecy.

Chaotic generators demonstrated high entropy values even on short time series, and their very long periods ensure the uniqueness of each sequence. The results confirmed the potential applicability of such generators in lightweight image encryption algorithms, which have shown resistance to cryptanalysis and efficiency in resource-constrained environments. The integration of chaotic maps, such as Henon and logistic maps, significantly expands the key space and increases the resistance to statistical attacks, making hybrid models a promising area of development. Chaotic generators can act as an additional source of entropy in modern cryptosystems, increasing their resilience and providing new directions for the development of information security theory and practice.

The limitation of the study was the theoretical nature and the lack of experimental verification of the results obtained, which requires further practical validation. Further research should focus on combining several chaotic maps, developing variable structures such as structure-varying CML, and expanding the range of tests, including the analysis of autocorrelation functions, min-entropy, and spectral characteristics.

Acknowledgements

None.

Funding

The study was not funded.

Conflict of Interest

None.

References

[1] Alghamdi, Y., Munir, A., & Ahmad, J. (2022). A lightweight image encryption algorithm based on chaotic map and random substitution. *Entropy*, 24(10), article number 1344. doi: 10.3390/e24101344.

[2] Al-Hyari, A., Abu-Faraj, M., Obimbo, C., & Alazab, M. (2025). Chaotic hénon-logistic map integration: A powerful approach for safeguarding digital images. *Journal of Cybersecurity and Privacy*, 5(1), article number 8. doi: 10.3390/jcp5010008.

[3] Ali, M., Ahmad, J., Khan, M.A.H., Ullah, S., Rehman, M.U., Shah, S.A., & Khan, M.S. (2025). A chaotic image encryption scheme using novel geometric block permutation and dynamic substitution. In F. Saeed, F. Mohammed, E. Mohhamed, S. Basura & M. Al-Sarem (Eds.), *Proceedings of the 4th international conference of advanced computing and informatics: Advances on intelligent computing and data science II* (pp. 1-12). Cham: Springer. doi: 10.1007/978-3-031-91351-8_1.

[4] Alibraheemi, H.M.M., Al Ibraheemi, M.M.A., & Radhy, Z.H. (2024). Design and practical implementation of a stream cipher algorithm based on a Lorenz system. *Journal of Information Security*, 4(3), 136-151. doi: 10.58496/MJCS/2024/019.

[5] Alloun, Y., Kifouche, A., Azzaz, M.S., Madani, M., Bourennane, E.-B., & Sadoudi, S. (2025). Design and FPGA implementation of a novel cryptographic secure pseudo random number generator based on artificial neural networks and chaotic systems. *Integration*, 103, article number 102388. doi: 10.1016/j.vlsi.2025.102388.

[6] Barker, E., & Kelsey, J. (2015). *Recommendation for random number generation using deterministic random bit generators*. Gaithersburg: U.S. Department of Commerce. doi: 10.6028/NIST.SP.800-90Ar1.

[7] Belazi, A., Kharbech, S., Aslam, N., Talha, M., Xiang, W., Iliyasu, A.M., & El-Latif, A.A.A. (2022). Improved Sine-Tangent chaotic map with application in medical images encryption. *Journal of Information Security and Applications*, 66, article number 103131. doi: 10.1016/j.jisa.2022.103131.
[8] Calderon, M.J.A., Lucas, L.J.L., Rosli, S.A.B., Ying, S.S.H., Lim, J.L.E., Xiang, M., & Teo, T.H. (2024). Logistic map pseudo random number generator in FPGA. *ArXiv*. doi: 10.48550/arXiv.2404.19246.
[9] Dhopavkar, T.A., Nayak, S.K., & Roy, S. (2022). IETD: A novel image encryption technique using tinkerbell map and duffing map for IoT applications. *Multimedia Tools and Applications*, 81, 43189-43228. doi: 10.1007/s11042-022-13162-x.
[10] Ding, P., Zhu, J., & Zhang, J. (2024). A four-dimensional no-equilibrium chaotic system with multi-scroll chaotic hidden attractors and its application in image encryption. *Physica Scripta*, 99, article number 105211. doi: 10.1088/1402-4896/ad7237.
[11] Faure, E., Shcherba, A., Skutskyi, A., & Lavdanskyi, A. (2024). A software model to generate permutation keys through a square matrix. *Bulletin of Cherkasy State Technological University*, 29(2), 10-23. doi: 10.62660/bcstu/2.2024.10.
[12] Fernández-Caramès, T.M., & Fraga-Lamas, P. (2020). Towards post-quantum blockchain: A review on blockchain cryptography resistant to quantum computing attacks. *IEEE Access,* 8, 21091-21116. doi: 10.1109/ACCESS.2020.2968985.
[13] Garipcan, A.M., Aydin, Y., & Özkaynak, F. (2025). An efficient 2D hyper chaos and DNA encoding-based s-box generation method using chaotic evolutionary improvement algorithm for nonlinearity. *Chaos, Solitons & Fractals*, 191, article number 115952. doi: 10.1016/j.chaos.2024.115952.
[14] Gençoğlu, M.T., Karaduman, Ö., & Özkaynak, F. (2025). Chaotic real number generator with quantum wave equation. *Symmetry*, 17(3), article number 349. doi: 10.3390/sym17030349.
[15] Gottschalk, W.H., & Hedlund, G.A. (1955). *Topological dynamics*. Providence: American Mathematical Society.
[16] Hadjadj, M.A., Kaibou, R., & Sadoudi, S. (2025). Design and hardware implementation of a prng-cs for embedded security applications. In *Proceedings of the 2025 IEEE computer society annual symposium on VLSI* (pp. 1-4). Los Alamitos: IEEE. doi: 10.1109/ISVLSI65124.2025.11130211.
[17] Irfan, M., & Khan, M.A. (2024). Cryptographically secure pseudo-random number generation (CS-PRNG) design using robust chaotic tent map (RCTM). *ArXiv*. doi: 10.48550/arXiv.2408.05580.
[18] Jackson, J., & Perumal, R. (2025). A robust image encryption technique based on an improved fractional order chaotic map. *Nonlinear Dynamics*, 113, 7277-7296. doi: 10.1007/s11071-024-10480-7.
[19] Knuth, D.E. (1969). *The art of computer programming*. Reading: Addison-Wesley.
[20] Krulikovskyi, O., Haliuk, S., Ivashko, V., & Politanskyi, R. (2024). Periodicity of timeseries generated by logistic map: Part II. *Security of Infocommunication Systems and Internet of Things*, 2(2), article number 02003. doi: 10.31861/sisiot2024.2.02003.
[21] Kumar, A., & Dua, M. (2021). Novel pseudo random key & cosine transformed chaotic maps based satellite image encryption. *Multimedia Tools and Applications*, 80, 27785-27805. doi: 10.1007/s11042-021-10970-5.
[22] Kumar, M., & Ch, D. (2025). Enhancing image security through a fusion of chaotic map and multi-level scrambling techniques. *Signal, Image and Video Processing*, 19, article number 235. doi: 10.1007/s11760-025-03814-4.
[23] Lorenz, E.N. (1963). Deterministic nonperiodic flow. *Journal of the Atmospheric Sciences*, 20(2), 130-141.
[24] Luo, Y., Fan, C., Xu, C., & Li, X. (2024). Design and FPGA implementation of a high-speed prng based on an n-D non-degenerate chaotic system. *Chaos, Solitons & Fractals*, 183, article number 114951. doi: 10.1016/j.chaos.2024.114951.
[25] Lyapunov, O.M. (1892). *General problem of stability of motion*. Kharkiv: Zilberberga's typography.
[26] Madouri, Z.B., Said, N.H., & Pacha, A.A. (2024). A new pseudorandom number generator based on chaos in digital filters for image encryption. *Journal of Optics*, 53, 3548-3563. doi: 10.1007/s12596-023-01606-y.
[27] May, R.M. (1976). Simple mathematical models with very complicated dynamics. *Nature*, 261, 459-467. doi: 10.1038/261459a0.
[28] Menezes, A.J., van Oorschot, P.C., & Vanstone, S.A. (2011). *Handbook of applied cryptography*. Boca Raton: CRC Press.
[29] Ming, H., Hu, H., & Zheng, J. (2023). Design and application of a structure-varying coupled chaotic system with high security. *Expert Systems with Applications*, 226, article number 120158. doi: 10.1016/j.eswa.2023.120158.
[30] Murillo-Escobar, D., Vega-Pérez, K., Murillo-Escobar, M.A., Arellano-Delgado, A., & López-Gutiérrez, R.M. (2024). Comparison of two new chaos-based pseudorandom number generators implemented in microcontroller. *Integration*, 96, article number 102130. doi: 10.1016/j.vlsi.2023.102130.
[31] Nazish, M., Javid, M., & Banday, M.T. (2025). Enhanced logistic map with infinite chaos and its applicability in lightweight and high-speed pseudo-random bit generation. *Cybersecurity*, 8, article number 24. doi: 10.1186/s42400-024-00319-4.
[32] Patidar, V., & Singh, T. (2025). A novel approach to pseudorandom number generation using hamiltonian conservative chaotic systems. *Frontiers in Physics*, 13, article number 1553389. doi: 10.3389/fphy.2025.1553389.
[33] Poincaré, H. (2017). *The three-body problem and the equations of dynamics: Poincaré's foundational work on dynamical systems theory.* Cham: Springer. doi: 10.1007/978-3-319-52899-1.

[34] Sambas, A., Benkouider, K., Kaçar, S., Ceylan, N., Vaidyanathan, S., Sulaiman, I.M., Mohamed, M.A., Ayob, A.F.M., & Muni, S.S. (2024). Dynamic analysis and circuit design of a new 3D highly chaotic system and its application to pseudo random number generator (PRNG) and image encryption. *SN Computer Science*, 5, article number 420. doi: 10.1007/s42979-024-02766-9.
[35] SHA-3 Standard: Permutation-based hash and extendable-output functions. (2015). doi: 10.6028/NIST.FIPS.202.
[36] Shandyba, A. (2025). *Method of embedding digital watermarks using chaotic maps*. Kharkiv: Kharkiv National University of Radioelectronics.
[37] Shannon, C.E. (1948). A mathematical theory of communication. *Bell System Technical Journal*, 27(3), 379-423. doi: 10.1002/j.1538-7305.1948.tb01338.x.
[38] Singh, P.K., Jha, B., & Kumar, S. (2024). An efficient and lightweight image encryption technique using Lorenz chaotic system. *Mathematical Modeling and Computing*, 11(3), 702-709. doi: 10.23939/mmc2024.03.702.
[39] Tiwari, A., Diwan, P., Diwan, T.D., Miroslav, M., & Samal, S.P. (2025). A compressed image encryption algorithm leveraging optimized 3D chaotic maps for secure image communication. *Scientific Reports*, 15, article number 14151. doi: 10.1038/s41598-025-95995-8.
[40] Yin, F., Li, A., Lv, C., Wu, R., & Gao, S. (2024). A new image encryption algorithm with feedback key mechanism using two-dimensional dual discrete quadratic chaotic map. *Nonlinear Dynamics*, 112, 20417-20435. doi: 10.1007/s11071-024-10099-8.

Застосування теорії хаосу для підвищення стійкості систем шифрування в інформаційних технологіях

Володимир Луханін

Кандидат фізико-математичних наук, асистент
Харківський національний університет радіоелектроніки
61166, просп. Науки, 14, м. Харків, Україна
https://orcid.org/0000-0003-4328-929X

Анотація. Метою дослідження було теоретичне обґрунтування застосування хаотичних динамічних систем для підсилення стійкості криптографічних ключів. Методологія дослідження базувалася на теоретичному, порівняльному та критичному аналізі наукових джерел для оцінки потенціалу хаотичних систем. Встановлено, що хаотичні карти забезпечують високу ентропію, довгі періоди та непередбачуваність згенерованих послідовностей завдяки чутливості до початкових умов, що підтверджується розрахунками ентропії Шеннона та позитивними Ляпуновськими показниками. Використання хеш-функцій та механізмів оновлення внутрішнього стану усуває статистичні кореляції й підвищує стійкість генераторів до криптоаналізу. Показано, що послідовності, отримані на основі логістичного відображення та системи Лоренца, проходять стандартні статистичні тести NIST SP 800-22, демонструючи рівномірність розподілу та відсутність кореляцій. Використання кола Чуа як аналогової схеми забезпечує фізично реалізовані генератори істинної випадковості (True Random Number Generator) з низьким енергоспоживанням, придатні для ресурсно-обмежених Internet of Things-систем. Схема з інтеграцією кількох хаотичних карт підтвердила збільшення простору ключів і підвищення стійкості до статистичних атак, у порівнянні з традиційними PseudoRandom Number Generator. Виявлено, що хаотичні генератори здатні забезпечити forward і backward secrecy завдяки оновленню внутрішнього стану системи, що запобігає повторюваності послідовностей. Хаотичні генератори мають переваги над традиційними завдяки дуже довгим періодам і чутливості до початкових умов, проте їх ефективність залежить від криптографічної постобробки та правильного вибору параметрів. Рекомендовано застосування хаотичних систем як додаткового джерела ентропії в програмних і апаратних реалізаціях, зокрема у легковагових криптографічних рішеннях для інтернету речей, сенсорних мереж і мобільних пристроїв. Практична значимість полягає у застосуванні результатів розробниками для безпечного шифрування, дослідниками для генерації випадкових чисел та інженерами інтернету речей для захисту пристроїв

Ключові слова: нелінійна динаміка; генератори випадкових чисел; криптографічна ентропія; хаотичні атрактори; ініціалізаційні вектори; топологічна транзитивність; криптографічна екстракція