IRSTI 20.53.23; 28.23.15; 28.23.29; 27.47.17 **https://doi.org/10.58805/kazutb.v.2.31-1722**

HYBRID ENCRYPTION ARCHITECTURE BASED ON CHAOTIC DYNAMICS AND AES-GCM ALGORITHM FOR PROTECTING MULTIMEDIA DATA

[1]A.T. Mazakova, [1]Sh.A. Jomartova✉, [2]A.L. Yessenbaeva, [1]A.A. Kulzhanova, [3]B. Zhao

[1]Al-Farabi Kazakh National University, Almaty, Kazakhstan,
[2]L.N.Gumilyov Eurasian National University, Astana, Kazakhstan,
[3]Dalian University of Technology, China

✉ *Corresponding author: jomartova@mail.ru*

This paper addresses the problem of secure encryption of images and binary data through the integration of chaotic dynamic systems and modern symmetric cryptographic primitives. The growing volume of multimedia data in telecommunication and information systems necessitates the development of encryption methods that ensure high resistance to statistical and differential cryptanalysis while accounting for the intrinsic structural properties of visual data.

A hybrid encryption algorithm is proposed, combining chaotic permutation and diffusion mechanisms with authenticated symmetric encryption based on the AES-256 algorithm in GCM mode. Chaotic sequences are generated using a logistic map, whose parameters are deterministically derived from key material via a key derivation function (Scrypt), enabling an expanded key space and high sensitivity to key variations. The algorithm implements a multi-stage transformation architecture, including chaotic preprocessing and subsequent authenticated encryption, ensuring both confidentiality and data integrity.

The performance and cryptographic properties of the proposed method are evaluated through numerical experiments on datasets of varying sizes and structures, including grayscale and color images, text, and binary files. The effectiveness of the algorithm is assessed using entropy analysis, histogram uniformity, and differential attack resistance metrics (NPCR and UACI). Experimental results demonstrate that the entropy of encrypted data approaches the theoretical maximum (≈8 bits per byte), indicating near-ideal randomness and elimination of statistical dependencies.

The proposed hybrid approach significantly enhances resistance to statistical and differential cryptanalysis compared to purely chaotic or classical cryptographic schemes. The results confirm the feasibility and effectiveness of integrating chaotic transformations with standardized cryptographic algorithms for secure multimedia data protection in modern information systems.

Keywords: chaotic sequences, image encryption, chaotic cryptography, permutation and diffusion, hybrid encryption algorithm, entropy, correlation analysis, information security, multimedia data protection.

МУЛЬТИМЕДИА ДЕРЕКТЕРІН ҚОРҒАУҒА АРНАЛҒАН ХАОТИКАЛЫҚ ДИНАМИКА ЖӘНЕ AES-GCM АЛГОРИТМІНЕ НЕГІЗДЕЛГЕН ГИБРИДТІК ШИФРЛАУ АРХИТЕКТУРАСЫ

[1]Ә.Т. Мазақова, [1]Ш.А. Жомартова✉, [2]А.Л. Есенбаева, [1]А.А. Кульжанова, [3]Б. Чжао

[1]Әл-Фараби атындағы Қазақ ұлттық университеті, Алматы, Қазақстан,
[2]Л.Н.Гумилев атындағы Еуразия ұлттық университеті, Астана, Қазақстан,
[3]Далянь технологиялық университеті, Қытай,
e-mail: jomartova@mail.ru

Бұл мақалада хаотикалық динамикалық жүйелер мен заманауи симметриялық криптографиялық примитивтерді біріктіру арқылы кескіндер мен екілік деректерді қауіпсіз шифрлау мәселесі қарастырылады. Телекоммуникация және ақпараттық жүйелердегі мультимедиялық деректердің көлемінің өсуі визуалды деректердің ішкі құрылымдық қасиеттерін ескере отырып, статистикалық және дифференциалды криптоталдауға жоғары төзімділікті қамтамасыз ететін шифрлау әдістерін әзірлеуді қажет етеді.

Хаотикалық пермутация және диффузия механизмдерін GCM режиміндегі AES-256 алгоритміне негізделген аутентификацияланған симметриялық шифрлаумен біріктіретін гибридті шифрлау алгоритмі ұсынылады. Хаотикалық тізбектер логистикалық картаны пайдаланып жасалады, оның параметрлері кілтті алу функциясы (Scrypt) арқылы кілт материалынан детерминирленген түрде алынады, бұл кеңейтілген кілт кеңістігін және кілт вариацияларына жоғары сезімталдықты қамтамасыз етеді. Алгоритм хаотикалық алдын ала өңдеуді және кейіннен аутентификацияланған шифрлауды қамтитын көп сатылы трансформация архитектурасын жүзеге асырады, бұл құпиялылықты да, деректердің тұтастығын да қамтамасыз етеді.

Ұсынылған әдістің өнімділігі мен криптографиялық қасиеттері сұр реңкті және түрлі-түсті кескіндерді, мәтінді және екілік файлдарды қоса алғанда, әртүрлі өлшемдер мен құрылымдардағы деректер жиынтықтарындағы сандық эксперименттер арқылы бағаланады. Алгоритмнің тиімділігі энтропия талдауы, гистограмманың біркелкілігі және дифференциалды шабуылға төзімділік көрсеткіштері (NPCR және UACI) арқылы бағаланады. Тәжірибелік нәтижелер шифрланған деректердің энтропиясының теориялық максимумға (байтқа ≈8 бит) жақындайтынын көрсетеді, бұл идеалға жақын кездейсоқтықты және статистикалық тәуелділіктердің жойылуын көрсетеді.

Ұсынылған гибридті тәсіл таза хаотикалық немесе классикалық криптографиялық схемалармен салыстырғанда статистикалық және дифференциалды криптоталдауға төзімділікті айтарлықтай арттырады. Нәтижелер қазіргі ақпараттық жүйелерде мультимедиялық деректерді қауіпсіз қорғау үшін хаотикалық түрлендірулерді стандартталған криптографиялық алгоритмдермен біріктірудің орындылығы мен тиімділігін растайды.

Түйін сөздер: Хаотикалық тізбектер, кескінді шифрлау, хаотикалық криптография, пермутация және диффузия, гибридті шифрлау алгоритмі, энтропия, корреляциялық талдау, ақпараттық қауіпсіздік, мультимедиялық деректерді қорғау.

ГИБРИДНАЯ АРХИТЕКТУРА ШИФРОВАНИЯ НА ОСНОВЕ ХАОТИЧЕСКОЙ ДИНАМИКИ И АЛГОРИТМА AES-GCM ДЛЯ ЗАЩИТЫ МУЛЬТИМЕДИЙНЫХ ДАННЫХ

[1]А.Т. Мазақова, [1]Ш.А. Джомартова✉, [2]А.Л. Есенбаева, [1]А.А. Кульжанова, [3]Б. Чжао

[1]Казахский национальный университет им. Аль-Фараби, Алматы, Казахстан,
[2]Евразийский национальный университет им. Л.Н.Гумилева, Астана, Казахстан,
[3]Даляньский технологический университет, Китай,
e-mail: jomartova@mail.ru

В данной статье рассматривается проблема безопасного шифрования изображений и бинарных данных путем интеграции хаотических динамических систем и современных симметричных криптографических примитивов. Растущий объем мультимедийных данных в телекоммуникационных и информационных системах требует разработки методов шифрования, обеспечивающих высокую устойчивость к статистическому и дифференциальному криптоанализу, при этом учитывающих внутренние структурные свойства визуальных данных.

Предложен гибридный алгоритм шифрования, сочетающий механизмы хаотической перестановки и диффузии с аутентифицированным симметричным шифрованием на основе алгоритма AES-256 в режиме GCM. Хаотические последовательности генерируются с использованием логистического отображения, параметры которого детерминированно выводятся из ключевого материала с помощью функции вывода ключа (Scrypt), что позволяет расширить ключевое пространство и обеспечить высокую чувствительность к изменениям ключа. Алгоритм реализует многоступенчатую архитектуру преобразования, включающую хаотическую предварительную обработку и последующее аутентифицированное шифрование, обеспечивая как конфиденциальность, так и целостность данных.

Производительность и криптографические свойства предложенного метода оцениваются с помощью численных экспериментов на наборах данных различного размера и структуры, включая изображения в оттенках серого и цветные изображения, текст и бинарные файлы. Эффективность алгоритма оценивается с помощью анализа энтропии, равномерности гистограммы и метрик устойчивости к дифференциальным атакам (NPCR и UACI). Экспериментальные результаты показывают, что энтропия зашифрованных данных приближается к теоретическому максимуму (≈8 бит на байт), что указывает на почти идеальную случайность и устранение статистических зависимостей.

Предложенный гибридный подход значительно повышает устойчивость к статистическому и дифференциальному криптоанализу по сравнению с чисто хаотическими или классическими криптографическими схемами. Результаты подтверждают осуществимость и эффективность интеграции хаотических преобразований со стандартизированными криптографическими алгоритмами для надежной защиты мультимедийных данных в современных информационных системах.

Ключевые слова: хаотические последовательности, шифрование изображений, хаотическая криптография, перестановка и диффузия, гибридный алгоритм шифрования, энтропия, корреляционный анализ, информационная безопасность, защита мультимедийных данных.

Introduction. With the rapid development of digital technologies and global digitalization, the volume of multimedia information transmitted, processed, and stored is growing significantly. A significant portion of this information flow consists of images and video data used in telecommunications systems, video surveillance systems, telemedicine, unmanned aerial and marine platforms, geographic information systems, biometric systems, intelligent monitoring systems, and machine vision. Visual information is increasingly being used not only as a display medium but also as a data source for automated decision-making systems, significantly increasing the requirements for its protection [1-6].

In modern information systems, ensuring the confidentiality, integrity, and authenticity of data is a key information security objective. Violating these properties in multimedia data can lead to the leakage of personal information, the substitution of visual data, the distortion of medical images, errors in navigation and monitoring systems, and the compromise of data in video surveillance systems and unmanned platforms. With the increasing number of cyberattacks and the development of data analysis methods, image protection issues are becoming increasingly important.

Classic cryptographic algorithms such as AES, DES, RSA, and their modifications were originally developed to protect general-purpose text and binary data. They are widely used in secure network protocols, banking and government information systems, electronic document management, and authentication systems. Despite their high formal cryptographic strength, these algorithms do not take into account the specific properties of images as the object of encryption. These properties include: 1) high correlation between adjacent pixels; 2) significant data redundancy; 3) two-dimensional spatial structure; 4) large volumes of information; 5) high sensitivity of visual perception to local distortions.

These characteristics mean that the direct application of standard block ciphers to images may not always be optimal in terms of computational efficiency, communication bandwidth, and resistance to specialized types of cryptanalysis aimed specifically at multimedia data. Furthermore, encrypting images without prior processing does not destroy their spatial structure, which in some cases can lead to statistical information leakage.

In this regard, specialized image encryption algorithms that take into account the statistical and structural properties of images have been actively developing in recent decades. The use of chaotic dynamic systems is of significant interest in this area. Chaotic systems are nonlinear dynamic systems possessing a number of fundamental properties that are particularly valuable for cryptographic applications: 1) sensitivity to initial

conditions (the “butterfly” effect); pseudorandom nature of trajectories; 2) ergodicity; 3) nonlinearity; 4) a high degree of phase space mixing [7-12].

Thanks to these properties, chaotic maps can be used as pseudorandom sequence generators, data permutation mechanisms, and diffusion schemes. The first works on the application of chaotic maps in cryptography demonstrated the fundamental possibility of constructing symmetric encryption algorithms based on one-dimensional and multidimensional chaotic maps. Subsequent studies proposed various chaotic models, including the logistic map, the Hénon map, the Chebyshev map, the PWLCM (Piecewise) map, and the symmetric-valued map. Linear Chaotic Map), Arnold cut-maps and their multidimensional generalizations.

Despite the large number of publications devoted to chaotic image encryption, a significant portion of the proposed algorithms have a number of significant drawbacks. The main problems include: 1) the lack of a rigorous cryptographic justification for security; 2) vulnerability to differential and statistical cryptanalysis; 3) small key space; 4) weak key sensitivity; 5) the lack of authentication and data integrity control mechanisms; 6) difficulties scaling to large images and streaming data [13-18].

In many studies, chaotic algorithms are evaluated primarily by empirical metrics (entropy, correlation, NPCR, UACI), without analyzing their robustness within a classical cryptographic adversary model. This limits the practical application of purely chaotic schemes in systems with high security requirements.

On the other hand, modern symmetric cryptographic algorithms, in particular the AES (Advanced Encryption Standard) possess a high degree of formal cryptographic strength, confirmed by years of analysis by the cryptographic community. AES is used in most secure network protocols (TLS, IPsec, VPN), in banking systems, and in government information infrastructures. However, classical block ciphers are not oriented toward the structural features of images and do not pre-mask spatial dependencies between pixels.

In this regard, the development of hybrid encryption algorithms that combine the advantages of chaotic methods and proven cryptographic standards is a pressing issue. This approach allows for: 1) use chaotic transformations to destroy the correlation and spatial structure of images; 2) apply standard cryptographic primitives to ensure formally provable cryptographic resistance; 3) implement authenticated encryption with data integrity control; 4) increase resistance to statistical and differential cryptanalysis.

Hybrid schemes allow us to eliminate the main shortcomings of purely chaotic algorithms and simultaneously expand the functionality of classical cryptosystems through preliminary chaotic data processing.

This paper focuses on the development and evaluation of a hybrid image encryption algorithm based on the integration of chaotic dynamic systems and the AES-256 symmetric cryptographic algorithm in GCM mode. The proposed algorithm implements a multi-layered security architecture, including chaotic permutation and diffusion of image pixels, as well as authenticated block encryption.

A logistic mapping is used as a chaotic sequence generator, the parameters of which are deterministically formed from the key material. The chaotic system is used to construct permutations of image rows and columns and to form a key matrix implementing the diffusion transform. After chaotic processing, the data is further encrypted using the AES-256-GCM algorithm, ensuring confidentiality and integrity control [19-23].

The aim of this work is to develop a cryptographically secure and practically applicable image encryption algorithm aimed at protecting visual information in modern telecommunication and information systems.

To achieve the stated goal, the following tasks are solved in the work: 1) analysis of modern methods of image encryption; 2) study of the properties of chaotic dynamic systems as applied to cryptographic applications; 3) development of the architecture of a hybrid encryption algorithm;

4) construction of a mathematical model of chaotic transformations; 5) software implementation of the algorithm; 6) study of the cryptographic properties of the proposed method based on numerical experiments.

The scientific novelty of the work lies in the development of a hybrid approach to image encryption, combining chaotic permutations and diffusion with authenticated symmetric encryption, as well as in the deterministic formation of parameters of a chaotic system from key material.

The practical significance of the work lies in the possibility of using the developed algorithm in secure channels for transmitting multimedia information, video surveillance systems, telemedicine platforms, unmanned systems, and intelligent monitoring systems.

Materials and methods. The objects of study in this paper were digital images and text files represented in byte form. The main types of input data were:

- halftone and color images in BMP and PNG formats;

- text files in TXT format;

- binary files of arbitrary structure.

Images were treated as two-dimensional luminance matrices (for grayscale images) or three-dimensional arrays of RGB components (for color images). To ensure the algorithm' s universality, all data was first converted to a one-dimensional byte sequence:

$$P = \{p_0, p_1, ..., p_{n-1}\}, \quad (1)$$

where n is the file length in bytes.

The key information was specified as an external key file containing a character or binary sequence of arbitrary length. The cryptographic key was generated using the Scrypt key derivation function, which ensures resistance to brute-force attacks and attacks using precomputed tables (rainbow tables).

Python 3.10-3.11 was used as the software platform, using the cryptography library, which implements the AES-256 algorithm in GCM mode. All experiments were conducted in a deterministic computing environment, ensuring reproducibility of the results.

Let the external key file be represented as a byte sequence:

$$K_{ext} = \{k_0, k_1, ..., k_{m-1}\}. \quad (2)$$

On its basis, cryptographic key material is formed:

$$K = Scrypt\left(K_{ext}, salt, r, n, p\right), \quad (3)$$

where $salt$ is a random salt, r, n, p are the parameters of the Scrypt function.

As a result, a 64-byte key material vector is formed:

$$K = \left(K_{AES}, K_{ch}\right), \quad (4)$$

where K_{AES} is a 256-bit key for the AES algorithm, K_{ch} is a subset of bytes used to generate the parameters of the chaotic system.

This approach provides: 1) an expansion of the key space; 2) protection against brute-force attacks; and 3) high sensitivity to changes in the key file.

The logistic mapping is used as the basic chaotic dynamic system:

$$x_{n+1} = \mu x_n \left(1 - x_n\right), \quad (5)$$

where $x_n \in (0, 1)$, $\mu \in (3.57, 4)$ is the parameter corresponding to the chaotic regime.

The initial value x_0 and parameter μ are formed deterministically from the key material K_{ch}:

$$x_0 = f_1(K_{ch}), \quad (6)$$

$$\mu = 3.57 + f_2\left(K_{ch}\right),$$

where f_1, f_2 are functions for mapping a bit sequence into real numbers.

To eliminate transient effects, "warming up" of the chaotic system is used:

$$x_{n+T} = F^T\left(x_0\right), \quad (7)$$

where T is the number of discarded initial iterations.

The pseudo-random sequence is formed according to the rule:

$k_n = \lfloor 256 * x_n \rfloor$,

which allows you to get a stream of bytes:

$K_{seq} = \{k_0, k_1, ..., k_{n-1}\}$.

Chaotic permutation method (confusion). To destroy the spatial structure of the original data, a chaotic permutation of array elements is used P.

Let' s define an array of indices:

$i = \{0, 1, ..., n-1\}$.

An auxiliary array is formed on the basis of a chaotic sequence:

$H = \{h_i\}$, $h_i = x_i$.

The permutation is constructed by sorting the indices in ascending order of values h_i:

$$\pi = argsort(H).$$

Then the permuted array is defined as:

$$P_i^{'} = P_{\pi(i)}. \quad (8)$$

This transformation destroys local correlation dependencies and provides spatial diffusion of data.

Chaotic diffusion method. After the permutation, a diffusion transform based on the XOR operation is applied:

$C_i = P_i^{'} \oplus K_{seq,i}$,

where $K_{seq,i}$ is an element of the chaotic key flow.

Diffusion ensures high sensitivity of the output data to changes in any byte of the input sequence or key, which meets the requirement of the avalanche effect in cryptography.

AES-256-GCM Authenticated Encryption Method. The sequence obtained after chaotic processing:

$$C^{'} = \{C_0, C_1, ..., C_{n-1}\}$$

is subjected to additional cryptographic encryption using the AES-256 algorithm in GCM mode:

$$C = AES - GCM(C^{'}, K_{AES}, nonce), \quad (9)$$

where *nonce* is a random initialization vector.

GCM mode provides: 1) data confidentiality; 2) integrity control; 3) protection against data substitution; 4) ciphertext authentication.

The structure of the output file is as follows:

$$Blob = \{salt, nonce, C, tag\}.$$

Decryption method. The decryption procedure is performed in reverse order:

1. Extraction *salt* and *nonce*.

2. Generation of key material K.

3. AES-GCM Decryption:
$C^{'} = AES_GCM^{-1}(C^{'}, K_{AES})$.

4. Back diffusion: $P_i^{'} = C_i \oplus K_{seq,i}$.

5. Reverse permutation: $P_i = P^{'}_{\pi^{-1}(i)}$.

The correctness of the recovery is ensured by the deterministic generation of chaotic parameters and permutations.

To analyze the cryptographic strength of the algorithm, entropy (Shannon) was used:

$$H = -\sum_{i=0}^{255} p_i \log_2 p_i \quad (10)$$

where p_i is the probability of occurrence of a byte with value i.

The computational complexity and execution time of the algorithm were also estimated.

Results and discussion. The purpose of the experimental study is to evaluate the performance and cryptographic strength of the proposed hybrid encryption algorithm for various types of data, including grayscale images, color images, text files, and binary data.

All experiments were conducted in Python 3.10-3.11 using the cryptography library. Test datasets

ranged from 64 KB to 4 MB, ensuring scalability analysis.

The correctness of the algorithm was verified using the following condition:

$$P = D(E(P, K), K), \quad (11)$$

where E and D denote encryption and decryption functions, respectively.

Experimental results confirmed that the original data is fully recovered without distortion, demonstrating the correctness and reliability of the proposed method.

To evaluate the randomness of encrypted data, Shannon entropy was calculated. The results are presented in Table 1.

Table 1 - Entropy of original and encrypted data

Data Type	Size (KB)	Original Entropy	Encrypted Entropy
Grayscale image	256	6.85	7.998
Color image	512	7.21	7.997
Text file	128	4.12	7.999
Binary file	1024	6.34	7.998

The entropy values of encrypted data are consistently close to the theoretical maximum of 8 bits per byte, indicating near-ideal randomness and absence of statistical patterns exploitable by attackers.

Histogram analysis was performed to evaluate the distribution of byte values before and after encryption. The results are presented in Table 2.

Table 2 - Histogram distribution characteristics

Data Type	Original Distribution	Encrypted Distribution
Grayscale image	Non-uniform	Uniform
Color image	Structured peaks	Uniform
Text file	Highly skewed	Uniform
Binary file	Semi-structured	Uniform

The uniform distribution observed in encrypted data confirms effective elimination of statistical dependencies, significantly reducing vulnerability to frequency-based attacks.

To assess resistance to differential cryptanalysis, NPCR (Number of Pixels Change Rate) and UACI (Unified Average Changing Intensity) metrics were calculated. The results are presented in Table 3.

Table 3 - Sensitivity metrics

Metric	Value
NPCR	99.62%
UACI	33.41%

The obtained values are close to ideal theoretical benchmarks (NPCR≈99.6%, UACI≈33%), demonstrating strong avalanche effect and high resistance to differential attacks. Table 4 - shows the comparative analysis results.

Table 4 - Comparison with existing metods

Method	Entropy	Correlation	Differential Resistance	Security Level
AES only	High	Medium	High	High
Chaos only	Medium	Low	Medium	Medium
Proposed method	High	Low	High	Very High

The hybrid approach combines the formal cryptographic strength of AES with the decorrelation capabilities of chaotic preprocessing, resulting in superior overall security.

Conclusion. The software implementation of the developed hybrid encryption algorithm is written in Python versions 3.10–3.11. This language was chosen due to the availability of advanced libraries for numerical computations and cryptographic operations, as well as the ease of experimental verification of the algorithms.

The software package implements a full cycle of cryptographic transformations and includes the following logical modules:

- data input and pre-processing module;
- key material generation module;
- chaotic sequence generation module;
- chaotic permutation (confusion) module;
- chaotic diffusion (diffusion) module;
- AES-256-GCM authenticated encryption module;
- inverse transform (decryption) module;
- statistical metrics calculation module (entropy).

The general scheme of software implementation corresponds to the following sequence:

$$P \to Chaos(P) \to AES - GCM \to C,$$

$$C \to AES - GCM^{-1} \to Chaos^{-1}(P) \to \hat{P}.$$

The correctness of the program' s operation is checked by the condition:

$$P = \hat{P}.$$

The goal of the numerical experiment is to test the performance and cryptographic properties of the developed algorithm for encrypting images and files based on chaotic sequences. The experiment aims to confirm the following properties of the algorithm:

- correctness of encryption and decryption procedures;
- high sensitivity to changes in input data and key;
- destruction of the statistical structure of the original data;
- resistance to statistical and differential cryptanalysis - acceptable computational efficiency.
- test files from 64 KB to 4 MB in size.

Computational experiments conducted allowed for a comprehensive evaluation of the cryptographic properties of the developed encryption algorithm, which is based on the use of chaotic sequences and permutation and diffusion operations. The results demonstrate the algorithm' s resistance to the main types of cryptanalysis and confirm its applicability for protecting images and files in byte representation.

Python Date 28/1/2026 Time 12:11

Name original misx.txt file

Encrypted file name mshifr.txt

Length of original file = 4001

Key file length = 276

Encrypted file length = 4052

Encryption time (in seconds) = 0

The name of the decrypted mshifr.txt

The name of the decrypted file is mrez.txt

Decryption time (in seconds) = 0

Experimental data show that the statistical characteristics of the ciphertext are virtually independent of the input file size and structure. This demonstrates the scalability of the proposed approach and its robustness when processing data of various types – from structured images to binary files of arbitrary formats.

Calculations of the encrypted data' s entropy show that its values in all experimental series are within a range close to the theoretical maximum value of 8 bits for byte data. This indicates a nearly uniform distribution of bytes in the ciphertext and the absence of any discernible statistical patterns.

In the context of cryptographic interpretation, this means that an attacker cannot obtain useful information about the structure of the original data based on frequency analysis of the ciphertext. Unlike original images and binary files, for which the byte distribution is significantly uneven, encrypted data exhibits properties close to random.

Thus, high entropy confirms the effectiveness of the applied chaotic transformations and diffusion operations in terms of destroying the statistical structure of the input data.

Compared to classical encryption algorithms without preprocessing, the proposed approach offers several advantages. On the one hand, it provides cryptographic properties comparable to modern standards (high entropy, lack of correlation, resistance to differential attacks). On the other hand, chaotic permutation and diffusion achieve additional destruction of the spatial structure of images.

Unlike purely chaotic encryption algorithms, which are often evaluated only by empirical metrics, the developed method relies on a formalized numerical scheme and demonstrates robust statistical properties on a wide range of test data.

Thus, the obtained results confirm the feasibility of a hybrid approach that combines the ideas of chaotic dynamics and classical cryptography.

Experimental results show that the algorithm' s computational complexity is primarily determined by the chaotic permutation step, implemented through sorting, and is O(NlogN). For file sizes up to several megabytes, the algorithm demonstrates acceptable execution time and can be used in practical image and file protection applications.

Литература

1. Адаменко М. Основы классической криптологии. Секреты шифров и кодов. – М.: Издательство «ДМК Пресс», 2023. - 297 с. ISBN 978-5-89818-556-5.

2. Аграновский, А.В. Практическая криптография: алгоритмы и их программирование. – М.: СОЛОН-Пресс, 2021. – 256 с. ISBN: 5-98003-002-6.

3. Sysoev V.V., Bykov A.Yu. Digital watermark processing algorithms for copyright protection of graphic files // Voprosy kiberbezopasnosti.- 2025. -Vol.5(69)- P.139-148. DOI 10.21681/2311-3456-2025-5-139-148.

4. Mazakova A., Jomartova Sh., Mazakov T., Brzhanov R., Gura D. The Use of Artificial Intelligence to Increase the Functional Stability of UAV // International Review if Aerospace Engineering (IREASE). -2024.- Vol.17(3). - P.98-106. DOI 10.15866/irease.v17i3.25067.

5. Mazakova A., Jomartova S., Mazakov T., Shormanov T., Amirkhanov B. Controllability of an unmanned aerial vehicle // IEEE 7th International Energy Conference (ENERGYCON). - 2022. - P.1-5. DOI 10.1109/ENERGYCON53164.2022.9830244.

6. Liu R., Dou X., Wang X., Li Q., Mazakov T. Marine moving target detection algorithm based on improved YOLOv8. Proc. SPIE 13780 // Second International Conference on Image Processing and Artificial Intelligence (ICIPAI 2025). – 2025. DOI 10.1117/12.3072475.

7. Бабаш А.В., Шанкин Г.П. Криптография. – М.: СОЛОН-Пресс, 2007. - 512 с. ISBN 5-93455-135-3.

8. Бернет С., Пэйн С. Криптография. – М.: БИНОМ, 2002. – 384 с.

9. Bauer F.L. Decrypted Secrets - Methods and Maxims of Cryptology. - Springer, 2007.- 4 p. ISBN 978-3-540-60418-1.

10. Граймс Р.А. Апокалипсис криптографии. Подготовка криптографии к квантовым вычислениям. – М.: ДМК Пресс, 2020. – 290 с. ISBN 978-5-97060-837-1.

11. Грибунин В.Г., Оков И.Н., Туринцев И.В. Цифровая стеганография. – М.: СОЛОН-Пресс, 2009. - 264 с. ISBN 5-98003-011-5.

12. Земор Ж. Курс криптографии. – М., Ижевск: Регулярная и хаотическая динамика, Институт компьютерных исследований, 2019. – 256 с. ISBN 5-93972-510-4.

13. Зубов А.Ю. Совершенные шифры. – М. Гелиос АРВ, 2003. – 160 с. ISBN 5-85438-076-5.

14. Зуйкова О.Л. Основы криптографической защиты информации. – М.: МИЭМ, 2005. – 207 с. ISBN 5-94506-122-0.

15. Ильин М.Е., Калинкина Т.И., Пржегорлинский В.Н. Криптографическая защита информации в объектах информационной инфраструктуры. – МДК «Криптографическая защита информации», 2026. – 288 с. ISBN 978-5-0054-4085-3.

16. Молдовян Н.А., Молдовян А.А. Введение в криптосистемы с открытым ключом. – СПб.: БХВ-Петербург, 2005. – 288 с. ISBN 5-94157-563-7.

17. Мао В. Современная криптография теория и практика. – М.:Вильямс, 2005. – 768с. ISBN 5-8459-0847-7.

18. Zolotareva I., Gorodinskaya I. Cryptographic methods of information protection. // Science & World, 2022. – P.1-5. DOI: 10.26526/2307-9401-2022-1-1-5

19. Michael N.J., Ogoegbulem O., Obukohwo V., Henry E.E. Number theory in rsa encryption systems // International Journal of Mathematics, 2023. – P.7-16. DOI:10.5281/zenodo.10209900

20. Кочергин В.И. Практика теории многомерных цифро-векторных множеств (криптология). – Томск : Издательство Томского университета, 2012. – 218 с.

21. Крэндалл Р., Померанс К. Простые числа: Криптографические и вычислительные аспекты. – М.: УРСС: Книжный дом «ЛИБРОКОМ», 2011. – 664 с.

22. Кутин В.Н., Молчанов В.А. Статистический анализ конечных групп и их применение в криптографии // XXIII Международная научно-техническая конференция «Технические средства защиты информации», 2025. – С. 201-205.

23. Нестеренко А.Ю. Теоретико-числовые методы в криптографии: учебное пособие. – Моск. гос. ин-т. электроники и математики, 2012. – 224 с.

References

1. Adamenko M. Osnovy klassicheskoj kriptologii. Sekrety shifrov i kodov. – M.: Izdatel’stvo «DMK Press», 2023. - 297 s. ISBN 978-5-89818-556-5. [in Russian]

2. Agranovskij, A.V. Prakticheskaja kriptografija: algoritmy i ih programmirovanie. – M.: SOLON-Press, 2021. – 256 c. ISBN 5-98003-002-6. [in Russian]

3. Sysoev V.V., Bykov A.Yu. Digital watermark processing algorithms for copyright protection of graphic files // Voprosy kiberbezopasnosti.- 2025. -Vol.5(69)- P. 139-148. DOI10.21681/2311-3456-2025-5-139-148.

4. Mazakova A., Jomartova Sh., Mazakov T., Brzhanov R., Gura D. The Use of Artificial Intelligence to Increase the Functional Stability of UAV // International Review if Aerospace Engineering (IREASE). -2024.- Vol.17(3). - P.98-106. DOI 10.15866/irease. v17i3.25067.

5. Mazakova A., Jomartova S., Mazakov T., Shormanov T., Amirkhanov B. Controllability of an unmanned aerial vehicle // IEEE 7th International Energy Conference (ENERGYCON). - 2022. - P.1-5. DOI 10.1109/ENERGYCON53164.2022.9830244.

6. Liu R., Dou X., Wang X., Li Q., Mazakov T. Marine moving target detection algorithm based on improved YOLOv8. Proc. SPIE 13780 // Second International Conference on Image Processing and Artificial Intelligence (ICIPAI 2025). – 2025. DOI 10.1117/12.3072475.

7. Babash A.V., Shankin G.P. Kriptografija. - M.: SOLON-Press, 2007. - 512 s. ISBN 5-93455-135-3. [in Russian]

8. Bernet S., Pjejn C. Kriptografija. -M.: BINOM, 2002. - 384 s. [in Russian]

9. Bauer F.L. Decrypted Secrets - Methods and Maxims of Cryptology. - Springer, 2007.- 4 p. ISBN 978-3-540-60418-1.

10. Grajms R.A. Apokalipsis kriptografii. Podgotovka kriptografii k kvantovym vychislenijam. - M.: DMK Press, 2020. - 290 s. ISBN 978-5-97060-837-1. [in Russian]

11. Gribunin V.G., Okov I.N., Turincev I.V. Cifrovaja steganografija. - M.: SOLON-Press, 2009. - 264 c. ISBN 5-98003-011-5. [in Russian]

12. Zemor Zh. Kurs kriptografii. - M., Izhevsk: Reguljarnaja i haoticheskaja dinamika, Institut komp’juternyh issledovanij, 2019. - 256 c. ISBN 5-93972-510-4. [in Russian]

13. Zibo A.Ju. Sovershennye shifry. - M. Gelios ARV, 2003. - 160 c. ISBN 5-85438-076-5. [in Russian]

14. Zujkova O.L. Osnovy kriptograficheskoj zashhity informacii. - M.: MIJeM, 2005. - 207 s. ISBN 5-94506-122-0. [in Russian]

15. Il’in M.E., Kalinkina T.I., Przhegorlinskij V.N. Kriptograficheskaja zashhita informacii v objektah informacionnoj infrastruktury. - MDK «Kriptograficheskaja zashhita informacii», 2026. - 283 c. ISBN 978-5-0054-4085-3. [in Russian]

16. Moldovjan N.A., Moldovjan A.A. Vvedenie v kriptosistemy s otkrytym kljuchom. – SPb.: BHVPeterburg, 2005. - 286 s. ISBN 5-94157-563-7. [in Russian]

17. Mao V. Sovremennaja kriptografija teorija i praktika. – M.: Vil’jams, 2005. - 768s. ISBN 5-8459-0847-7. [in Russian]

18. Zolotareva I., Gorodinskaya I. Cryptographic methods of information protection. // Science & World, 2022. - P. 1-5. DOI 10.26526/2307-9401-2022-1-1-5.

19.Michael N.J., Ogoegbulem O., Obukohwo V., Henry E.E. Number theory in rsa encryption systems // International Journal of Mathematics.- 2023.- Vol.6(11)- P. 7-16. DOI 10.5281/zenodo.10209900.

20. Kochergin V.I. Praktika teorii mnogomernyh cifro-vektornyh mnozhestv (kriptologija). – Tomsk : Izdatel’stvo Tomskogo universiteta, 2013. - 217 s. ISBN 978-5-7511-2072-7. [in Russian]

21. Krjendall R., Pomerans K. Prostye chisla: Kriptograficheskie i vychislitel’nye aspekty. - M.: URSS: Knizhnyj dom «LIBROKOM», 2011. -664 c. ISBN 978-5-453-00016-6. [in Russian]

22. Kutin V.N., Molchanov V.A. Statisticheskij analiz konechnyh grupp i ih primenenie v kriptografii

// XXIII Mezhdunarodnaja nauchno-tehnicheskaja konferencija «Tehnicheskie sredstva zashhity informacii», 2025. - S. 201-205. [in Russian]

23. Nesterenko A.Ju. Teoretiko-chislovye metody v kriptografii: uchebnoe posobie. - Mosk. gos. in-t. jelektroniki i matematiki, 2012. - 224 s. ISBN 978-5-94506-320-4. [in Russian]

Author information

Mazakova A.- PhD, senior lecturer at al-Farabi KazNU, Almaty, Kazakhstan, e-mail: aigerym97@mail.ru;

Jomartova Sh.- Doctor of Technical Sciences, Professor of Al-Farabi KazNU, Almaty, Kazakhstan, e-mail: jomartova@mail.ru;

Yessenbaeva A.- doctoral student at L.N. Gumilyov ENU, Astana, Kazakhstan, e-mail: Yessenbaeva@mail.ru;

Kulzhanova A.- doctoral student at Al-Farabi KazNU, Almaty, Kazakhstan, e-mail: akbota.kulzhanova1594@gmail.com;

Zhao Baidong- Senior Lecturer, Dalian Polytechnic University, China, Dalian, e-mail: xiaoyuezhishang@vip.qq.com.

Сведения об авторах

Мазақова Ә.Т. - PhD, старший преподаватель КазНУ имени аль-Фараби, Алматы, Казахстан, e-mail: aigerym97@mail.ru;

Джомартова Ш.А.- д.т.н., профессор КазНУ имени аль-Фараби, Алматы, Казахстан,e-mail: jomartova@mail.ru;

Есенбаева А.Л.- докторант ЕНУ имени Л.Н. Гумилева, Астана, Казахстан, e-mail: Yessenbaeva@mail.ru;

Кульжанова А.А.- докторант КазНУ имени аль-Фараби, Алматы, Казахстан, e-mail: akbota.kulzhanova1594@gmail.com;

Чжао Байдун – старший преподаватель, Даляньский политехнический университет,Далянь, Китай, e-mail: xiaoyuezhishang@vip.qq.com.