https://doi.org/10.58805/itamns.V.1(32)-29

MODIFIED IMAGE ENCRYPTION ALGORITHM BASED ON CHAOTIC DYNAMICS

A.T. Mazakova[1], Sh.A. Jomartova[1]✉, A.L.Yessenbaeva[2], A.D.Mailybaeva[3], B.Zhao[4]

[1] *Al-Farabi Kazakh National University, Almaty, Kazakhstan*
[2] *L.N.Gumilyov Eurasian National University, Astana, Kazakhstan*
[3] *Kh. Dosmukhamedov Atyrau University, Atyrau, Kazakhstan*
[4] *Dalian University of Technology, Dalian, China*
✉ *Corresponding author: jomartova@mail.ru*

Received: 29 July 2026
Accepted: 05 September 2026
Published: 30 September 2026
Citation: Sh.A. Jomartova, et al. « MODIFIED IMAGE ENCRYPTION ALGORITHM BASED ON CHAOTIC DYNAMICS ». Information Technologies, Automation, and Management in Natural Sciences, vol. 1, no. 32, Sept. 2026, doi: https://doi.org/10.58805/itamns.V.1(32)-29
License CC BY 4.0

This article examines the development of a modified image encryption algorithm based on chaotic dynamics. The relevance of the study lies in the fact that in modern telecommunications, medical, biometric, monitoring, and information systems, digital images often contain confidential data and require reliable protection against unauthorized access, substitution, and distortion. Furthermore, images possess specific properties that distinguish them from ordinary text and binary data: high correlation between adjacent pixels, significant redundancy, a two-dimensional spatial structure, and a large volume of information. For this reason, the direct application of traditional cryptographic algorithms does not always effectively disrupt the statistical structure of an image.

This study is based on a hybrid approach combining chaotic transformations and standard cryptographic mechanisms. The core architecture utilizes chaotic permutation, diffusion, and subsequent authenticated AES-256-GCM encryption. This approach leverages the advantages of chaotic systems for pixel pre-shuffling and the advantages of AES-GCM for ensuring confidentiality, integrity, and data authentication. This paper proposes a modification of the algorithm based on the use of two chaotic mappings: a logistic mapping and a tent mapping. The logistic mapping is used to generate a global permutation sequence, while the tent mapping is used for block shuffling and diffusion flow generation. Additionally, the algorithm incorporates a key-dependent block permutation and double feedback diffusion. The first diffusion modifies pixel values using a chaotic pseudorandom flow, while the second creates a chain-like dependency between ciphertext bytes. This allows a change in a single pixel of the original image or a minor change in the secret key to significantly alter the final encrypted image. The key material is generated using the Scrypt function and is divided into several parts, each for AES-256-GCM, logistic mapping parameters, tent mapping parameters, block permutation, and feedback. This division increases the algorithm's sensitivity to the key and ensures the independence of individual encryption stages. To evaluate the effectiveness of the proposed algorithm, entropy, adjacent pixel correlation, histogram analysis, NPCR, and UACI metrics are used. The proposed modification is expected to improve the uniformity of pixel distribution in the encrypted image, reduce the correlation between adjacent pixels, enhance the avalanche effect, and improve resistance to statistical and differential cryptanalysis. The proposed algorithm can be used to protect images in video surveillance systems, telemedicine, biometric identification, intelligent monitoring, and secure telecommunications services.

Keywords: chaotic dynamics, image encryption, logistic mapping, tent mapping, chaotic permutation, diffusion, AES-GCM, information security, NPCR, UACI.

ХАОТИКАЛЫҚ ДИНАМИКАҒА НЕГІЗДЕЛГЕН МҰДІРЛЕНГЕН БЕЙНЕ ШИФРЛАУ АЛГОРИТМІ

Ә.Т.Мазақова[1], Ш.А. Жомартова[1]✉, А.Л.Есенбаева[2], А.Д Майлыбаева[3], Б.Чжао[4]

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

Мақалада хаотикалық динамикаға негізделген өзгертілген кескінді шифрлау алгоритмін жасау мәселесі қарастырылады. Зерттеудің өзектілігі қазіргі заманғы телекоммуникациялар, медициналық, биометриялық, мониторингтік және ақпараттық жүйелерде цифрлық кескіндер көбінесе құпия деректерді қамтиды және рұқсат етілмеген қол жеткізуден, ауыстырудан және бұрмалаудан сенімді қорғауды талап ететіндігімен түсіндіріледі. Сонымен қатар кескіндердің кәдімгі мәтіннен және екілік деректерден ерекшеленетін спецификалық қасиеттері бар: көрші пикселдер арасындағы жоғары корреляция, маңызды артықтық, екі өлшемді кеңістіктік құрылым және ақпараттың үлкен көлемі. Осы себепті дәстүрлі криптографиялық алгоритмдерді тікелей қолдану кескіннің статистикалық құрылымын тиімді жоюды әрқашан қамтамасыз ете бермейді. Зерттеудің негізі ретінде хаотикалық түрлендірулер мен стандартты криптографиялық механизмдерді біріктіретін гибридті тәсіл пайдаланылды. Негізгі архитектура кездейсоқ ауыстыруды, диффузияны және кейінгі аутентификацияланған AES-256-GCM шифрлауын пайдаланады. Бұл тәсіл пикселдерді алдын ала араластыру үшін хаотикалық жүйелердің артықшылығын және деректердің құпиялылығын, тұтастығын және аутентификациясын қамтамасыз ету үшін AES-GCM артықшылықтарын пайдаланады. Бұл жұмыс екі ретсіз бейнелеуді қолдануға негізделген алгоритмнің модификациясын ұсынады: логистикалық карта және шатыр картасы. Логистикалық карталау жаһандық ауыстыру тізбегін құру үшін пайдаланылады, ал шатыр картасы блоктарды араластыру және диффузиялық ағынды генерациялау үшін қолданылады. Сонымен қатар, алгоритмге кілтке тәуелді блок ауыстыру және кері байланыспен қосарланған диффузия енгізілген. Бірінші диффузия хаотикалық псевдокездейсоқ ағынды пайдалана отырып, пиксель мәндерін өзгертеді, ал екіншісі шифрленген мәтін байттары арасындағы тізбекті қатынасты құрайды. Осының арқасында бастапқы кескіннің бір пикселін өзгерту немесе құпия кілттің сәл өзгеруі соңғы шифрланған кескіннің айтарлықтай өзгеруіне әкеледі. Негізгі материал Scrypt функциясы арқылы жасалады және AES-256-GCM, логистикалық карта параметрлері, шатырды кескіндеу параметрлері, блок ауыстыру және кері байланысқа арналған бірнеше бөліктерге бөлінеді. Бұл бөлу алгоритмнің кілтке сезімталдығын арттырады және жеке шифрлау кезеңдерінің тәуелсіздігін қамтамасыз етеді. Ұсынылған алгоритмнің тиімділігін бағалау үшін энтропия көрсеткіштерін, көрші пикселдердің корреляциясын, гистограммалық талдауды, NPCR және UACI қолдану қарастырылған. Ұсынылған модификация шифрланған кескіндегі пиксельдердің таралуының біркелкілігін жақсартады, көрші пикселдер арасындағы корреляцияны азайтады, көшкін әсерін күшейтеді, статистикалық және дифференциалды криптоталдауға төзімділікті арттырады деп күтілуде. Ұсынылған алгоритм бейнебақылау жүйелеріндегі, телемедицинадағы, биометриялық сәйкестендірудегі, интеллектуалды бақылаудағы және қауіпсіз телекоммуникация қызметтеріндегі кескіндерді қорғау үшін пайдаланылуы мүмкін.

Түйін сөздер: хаотикалық динамика, кескінді шифрлау, логистикалық картаға түсіру, шатыр картаға түсіру, хаотикалық пермутация, диффузия, AES-GCM, ақпараттық қауіпсіздік, NPCR, UACI.

МОДИФИЦИРОВАННЫЙ АЛГОРИТМ ШИФРОВАНИЯ ИЗОБРАЖЕНИЙ НА ОСНОВЕ ХАОТИЧЕСКОЙ ДИНАМИКИ

Ә.Т. Мазақова[1], Ш.А Джомартова[1]✉, А.Л. Есенбаева[2], А.Д. Майлыбаева[3], Б.Чжао[4]

[1] Казахский национальный университет имени Аль-Фараби, Алматы, Казахстан
[2] Евразийский национальный университет имени Л.Н.Гумилева, Астана, Казахстан
[3] Атырауский университет им. Х. Досмухамедова, Атырау, Казахстан
[4] Даляньский технологический университет, Далянь, Китай
✉ *e-mail:jomartova@mail.ru*

В статье рассматривается задача разработки модифицированного алгоритма шифрования изображений на основе хаотической динамики. Актуальность исследования обусловлена тем, что в современных телекоммуникационных, медицинских, биометрических, мониторинговых и информационных системах цифровые

изображения часто содержат конфиденциальные данные и требуют надежной защиты от несанкционированного доступа, подмены и искажения. При этом изображения обладают специфическими свойствами, отличающими их от обычных текстовых и бинарных данных: высокой корреляцией между соседними пикселями, значительной избыточностью, двумерной пространственной структурой и большим объемом информации. По этой причине прямое применение традиционных криптографических алгоритмов не всегда обеспечивает эффективное разрушение статистической структуры изображения. В качестве основы исследования использован гибридный подход, объединяющий хаотические преобразования и стандартные криптографические механизмы. В архитектуре [1] применяются хаотическая перестановка, диффузия и последующее аутентифицированное шифрование AES-256-GCM. Такой подход позволяет использовать преимущества хаотических систем для предварительного перемешивания пикселей и преимущества AES-GCM для обеспечения конфиденциальности, целостности и аутентификации данных. В данной работе предложена модификация алгоритма, основанная на применении двух хаотических отображений: логистического отображения и тент-отображения. Логистическое отображение используется для формирования последовательности глобальной перестановки, а тент-отображение применяется для блочного перемешивания и генерации диффузионного потока. Дополнительно в алгоритм введены ключезависимая блочная перестановка и двойная диффузия с обратной связью. Первая диффузия изменяет значения пикселей с использованием хаотического псевдослучайного потока, а вторая формирует цепную зависимость между байтами шифротекста. Благодаря этому изменение одного пикселя исходного изображения или незначительное изменение секретного ключа приводит к существенному изменению итогового зашифрованного изображения. Ключевой материал формируется с использованием функции Scrypt и разделяется на несколько частей, предназначенных для AES-256-GCM, параметров логистического отображения, параметров тент-отображения, блочной перестановки и обратной связи. Такое разделение повышает чувствительность алгоритма к ключу и обеспечивает независимость отдельных этапов шифрования. Для оценки эффективности предложенного алгоритма предусматривается использование показателей энтропии, корреляции соседних пикселей, анализа гистограмм, NPCR и UACI. Ожидается, что предложенная модификация позволит повысить равномерность распределения пикселей зашифрованного изображения, снизить корреляцию между соседними пикселями, усилить лавинный эффект и повысить устойчивость к статистическому и дифференциальному криптоанализу.

Предложенный алгоритм может быть использован для защиты изображений в системах видеонаблюдения, телемедицине, биометрической идентификации, интеллектуальном мониторинге и защищенных телекоммуникационных сервисах.

Ключевые слова: хаотическая динамика, шифрование изображений, логистическое отображение, тент-отображение, хаотическая перестановка, диффузия, AES-GCM, информационная безопасность, NPCR, UACI.

Introduction. In today's digitalized world, images have become one of the most widespread and significant forms of multimedia information. They are used in telecommunications systems, video surveillance, medical diagnostics, biometric identification, geoinformation services, unmanned aerial vehicles, intelligent monitoring systems, educational platforms, and machine vision systems. Unlike traditional text data, images contain not only formal information but also visual features that allow for the identification of objects, people, technical conditions, medical pathologies, and other important data. Therefore, a breach of confidentiality, integrity, or authenticity of images can lead to the leakage of personal data, distortion of diagnostic results, compromise of surveillance systems, and the substitution of data in automated decision-making systems [1, 2].

The growing volume of transmitted and stored images increases the need for their protection. In modern information systems, images are often transmitted over open communication channels, stored in cloud storage, used in mobile applications, and processed by intelligent algorithms. Under these conditions, an attacker can not only gain unauthorized access to an image but also modify, replace, or analyze it to extract hidden information. Therefore, the task of reliable image encryption is relevant for both scientific research and practical information security systems [3, 4].

Classic cryptographic algorithms such as AES, DES, RSA, and their modifications are widely used to protect text and binary data. They possess high cryptographic

strength and are employed in secure network protocols, banking systems, electronic document management, and government information resources [5, 6]. However, the direct application of traditional encryption algorithms to images is not always optimal. This is due to the fact that digital images have specific properties that distinguish them from regular files. These properties include high correlation between adjacent pixels, significant data redundancy, a two-dimensional spatial structure, and a large volume of information [7, 8].

In most natural images, adjacent pixels have similar brightness or color values. For example, solid-color areas, object contours, background areas, and smooth transitions form stable spatial dependencies. If these dependencies are not specifically broken before encryption, the statistical structure of the original image may in some cases be partially preserved. Therefore, when developing image encryption algorithms, it is necessary to consider not only the general requirements of cryptographic protection but also the specific characteristics of visual data [9].

A reliable image encryption algorithm must ensure several key properties. First, the encrypted image should not visually resemble the original image. Second, the distribution of pixel values in the encrypted image should be nearly uniform. Third, the correlation between adjacent pixels should approach zero. Fourth, the algorithm must be highly sensitive to changes in the secret key and the original image. Even a change in a single pixel or a single bit of the key should significantly alter the encrypted result. These requirements are related to the need for protection against statistical and differential cryptanalysis [10, 11].

One promising area of image security is the use of chaotic dynamic systems. Chaotic systems are nonlinear dynamic models whose behavior is characterized by high sensitivity to initial conditions, pseudo-randomness of trajectories, ergodicity, and the ability to intensively mix phase space [12]. Even a slight change in the initial value or control parameter can lead to the formation of a completely different sequence of states. This property is called the "initial condition sensitivity effect" and is one of the reasons for the widespread use of chaotic dynamics in cryptographic problems.

In the context of image encryption, chaotic mappings can be used to construct pixel permutations, generate pseudorandom sequences, and implement diffusion transformations. A permutation alters pixel positions and destroys the spatial structure of an image, while diffusion modifies pixel values so that a change in one element of the original image affects many elements of the ciphertext. These two principles correspond to the classical cryptographic ideas of mixing and diffusion, formulated by K. Shannon in the theory of secrecy systems [2].

A large number of image encryption algorithms based on chaotic mappings have been proposed in the scientific literature. Among them, methods using the logistic mapping, the Henon mapping, the Arnold mapping, the Chebyshev mapping, piecewise linear chaotic mappings, and multidimensional chaotic systems [7-10] stand out. For example, the logistic mapping is often used due to its ease of implementation and ability to generate pseudorandom sequences in a chaotic regime. The Arnold mapping is used to permutate image pixels, and multidimensional chaotic maps allow for increasing the complexity and dimensionality of the key space [8].

Despite significant interest in chaotic cryptography, purely chaotic algorithms have a number of limitations. Many studies evaluate the security of such algorithms primarily using empirical metrics such as entropy, neighboring pixel correlation, NPCR, and UACI. These metrics are important for analyzing the quality of image encryption; however, they do not always provide a complete assessment of cryptographic strength within the classical adversary model [11]. Furthermore, some chaotic algorithms may have insufficiently large key spaces, weak key sensitivity, dependence on floating-point precision, and lack a built-in data integrity mechanism [3, 11].

On the other hand, modern standard cryptographic algorithms, particularly AES, possess high formal security and have a long history of practical use. AES is used in secure communication protocols, VPN systems, banking applications, and government information infrastructures [5]. Of particular importance is the AES-GCM mode, which ensures not only confidentiality but also data authentication. This means that the recipient can verify whether the encrypted data has been altered or tampered with during transmission [6]. This is especially important for protecting images, as an attacker can not only attempt to restore the original image but also surreptitiously alter its contents.

In this regard, a hybrid approach combining chaotic transformations and standard cryptographic mechanisms is of particular interest. This approach utilizes chaotic dynamics as a preprocessing step in the image: pixel permutation, spatial structure destruction, and value diffusion are performed. The result is then

further encrypted using a cryptographically secure algorithm, such as AES-256-GCM. This approach combines the advantages of chaotic systems and proven cryptographic primitives.

The paper [1], on which this study is based, proposes a hybrid architecture for multimedia data encryption that combines chaotic permutation, chaotic diffusion, and AES-256-GCM. In this architecture, chaotic sequences are generated using a logistic map, and the parameters of the chaotic system are deterministically derived from the key material using the Scrypt function. This approach allows for an expansion of the key space and increases the sensitivity of the algorithm to key changes. The paper [1] also notes that the algorithm's performance is evaluated using entropy, histogram uniformity, NPCR, and UACI, and the results show that the entropy of encrypted data approaches the theoretical maximum of approximately 8 bits per byte. However, the approach [1] can be further strengthened by expanding the chaotic part of the algorithm. Using only one logistic mapping can limit the diversity of generated sequences and make the algorithm dependent on the properties of a single chaotic map.

Furthermore, a single permutation and a single diffusion step do not always ensure maximum destruction of local image dependencies. Therefore, in this paper, we propose a modified algorithm that uses two chaotic systems: the logistic mapping and the tent mapping.

The proposed algorithm uses a logistic mapping to generate a global permutation sequence. It allows for reordering pixels throughout the image, destroying its original spatial structure. A tent mapping is used for block shuffling and diffusion flow generation. This separation of functions between two chaotic systems increases the independence of the algorithm's stages and complicates the recovery of patterns in encrypted data.

Additionally, a key-dependent block permutation is introduced into the algorithm. After global shuffling, the image is divided into blocks, within which an additional chaotic permutation is performed. The block size depends on the key material, making the shuffling structure unique for each secret key. This approach is aimed at eliminating local statistical dependencies that may persist after global shuffling.

Another important element of the modification is double diffusion with feedback. The first diffusion modifies pixel values using a chaotic pseudorandom stream. The second diffusion creates a chain dependence between ciphertext bytes, in which each current byte depends on the previous encrypted value. This achieves an enhanced avalanche effect: changing a single pixel in the original image or a minor change in the secret key leads to significant changes in the final encrypted image. This increases the algorithm's resistance to differential cryptanalysis [10, 11].

The relevance of this study stems from the need to develop algorithms that take into account the specific characteristics of digital images while simultaneously employing robust cryptographic mechanisms. Standard encryption alone may be insufficient to pre-destroy the visual structure of an image, while chaotic dynamics alone may not provide the required level of cryptographic rigor and integrity control. Therefore, a hybrid approach supplemented with modified chaotic transformations is a viable direction for research.

The aim of this work is to develop a modified image encryption algorithm based on chaotic dynamics, which provides increased resistance to statistical and differential cryptanalysis through the combined use of logistic mapping, tent mapping, key-dependent block permutation, double diffusion and AES-256-GCM.

To achieve this goal, it is necessary to solve the following tasks: consider the features of digital images as an object of cryptographic protection; analyze the possibilities of using chaotic dynamics for image encryption; develop a modified algorithm structure based on two chaotic mappings; propose a mechanism for global and block pixel permutation; develop a double diffusion scheme with feedback; determine the performance evaluation indicators of the algorithm, including entropy, correlation, NPCR, UACI and histogram analysis; justify the advantages of the proposed approach compared to a hybrid architecture.

The object of this research is digital images represented as pixel matrices or one-dimensional byte sequences. The subject of this research is methods of chaotic image encryption based on permutation, diffusion, and hybrid applications of standard cryptographic algorithms.

Thus, developing a modified image encryption algorithm based on chaotic dynamics is a relevant and practically significant task. The proposed approach combines the advantages of chaotic transformations and standard authenticated encryption, thereby improving the security of visual information in modern digital systems.

Materials and methods. The object of the study is digital images represented as pixel matrices. Grayscale and color images in PNG, BMP, or JPEG formats can be

used as input data. For universal processing, the image is converted into a one-dimensional byte sequence:

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

where is the p_i-th $i$byte of the original image, $n$is the length of the image in bytes.

A color image is processed using three components: R, G, and B. Each component can be processed separately, or all components can be combined into a single byte sequence. In the latter case, the algorithm becomes universal and can be applied not only to images but also to arbitrary binary data.

The external secret key is used as key information:

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

Based on this, extended key material is generated using the Scrypt function:

$$K = Scrypt(K_{ext}, salt, r, n, p), \quad (2)$$

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

The obtained key material is divided into four parts:

$$K = (K_{AES}, K_{ch1}, K_{ch2}, K_{fb}), \quad (3)$$

where $K_{AES}$is the key for AES-256-GCM; K_{ch1} are the logistic mapping parameters; $K_{ch2}$are the tent mapping parameters; $K_{fb}$are the block permutation and feedback parameters.

The article [1] also uses Scrypt , which allows for the deterministic generation of chaotic system parameters from key material and increases the algorithm's sensitivity to key changes. The proposed modification retains this approach, but additionally divides the key material between several encryption stages, as shown in Figure 1.

At the first stage, a chaotic sequence is formed using a logistic mapping:

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

where $x_n \in (0, 1)$, $\mu$is the control parameter of the chaotic system.

The initial value $x_0$and parameter $\mu$are determined from the key material:

$$x_0 = f_1(K_{ch}), \quad (4)$$
$$\mu = 3.57 + 0.43 * f_2(K_{ch}).$$

The sequence $X = \{x_0, x_1, ..., x_{n-1}\}$is used to globally permute pixels.

In the second stage, tent mapping is additionally used to enhance the chaotic properties of the algorithm:

$$y_{n+1} = \begin{cases} \alpha * y_n, & \text{if } y_n < 0.5 \\ \alpha(1 - y_n), & \text{if } y_n \geq 0.5 \end{cases} \quad (5)$$

The display parameters are set as follows:

$$y_0 = f_3(K_{ch2}), \quad (6)$$
$$\alpha = 1.9 + 0.1 * f_4(K_{ch2}).$$

The sequence $Y = \{y_0, y_1, ..., y_{n-1}\}$is used for block rearrangement and diffusion flow formation.

To eliminate the influence of the initial transient process, the first Tvalues of the chaotic sequences are discarded:

$$T = 1000 + (K_{fb} \bmod 500). \quad (7)$$

After preprocessing, working chaotic sequences X and Y are formed, the length of which corresponds to the length of the original byte sequence.

Based on the sequence X, an array of indices is constructed:

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

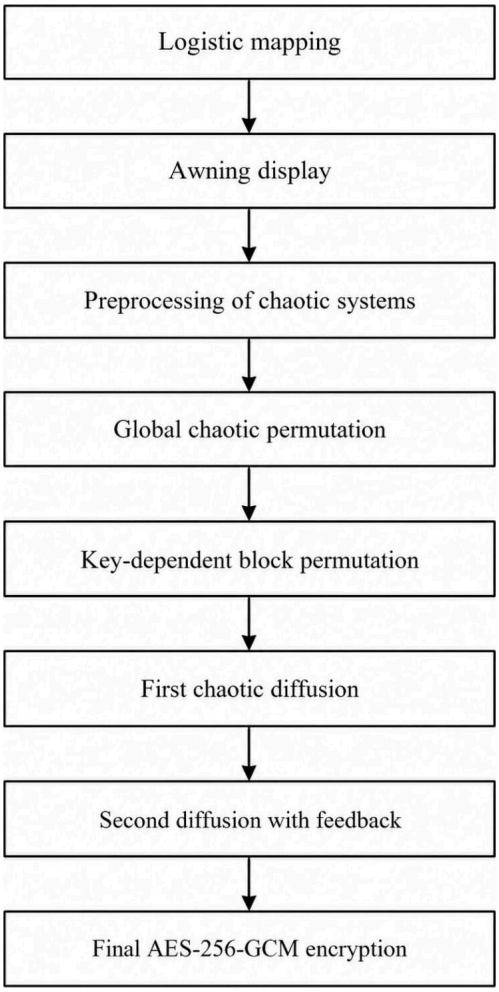


Fig. 1 - Scheme of encryption stages

Then the indices are sorted by the values of the chaotic sequence:

$$\pi = argsort(X). \quad (8)$$

After this, the original sequence is permuted:

$$P_i^{'} = P_{\pi(i)}. \quad (9)$$

This stage destroys the spatial structure of the image and reduces the correlation between adjacent pixels.

After the global permutation, the sequence P' is divided into blocks of length L:

$$L = 256 + (K_{fb} \bmod 768). \quad (10)$$

Thus, the block size can vary from 256 to 1024 bytes. Within each block, an additional permutation is performed based on fragments of the Y sequence:

$$B_i' = Permute(B_i, Y_i) \quad (11)$$

The introduction of block permutation allows us to further break local dependencies that may persist after global shuffling.

Based on the tent mapping, a pseudo-random byte stream is generated:

$$S_i = \lfloor 256 * y_i \rfloor$$

Then the XOR operation is performed:

$$C_i^{(1)} = P_i'' \oplus S_i \quad (12)$$

where P_i'' is the byte after global and block permutation.

To enhance the avalanche effect, a second diffusion is used:

$$C_i^{(2)} = C_i^{(1)} \oplus C_{i-1} \oplus R_i, \quad (13)$$

where

$$R_i = \lfloor 256 * x_i \rfloor$$

The first byte is assigned an initial value:

$$C_{-1}^{(2)} = IV_{ch}$$

The parameter IV_{ch} is formed from a part of the key K_{fb}.

This stage ensures that each subsequent byte of the ciphertext depends on the previous result, which increases the sensitivity of the algorithm to small changes in the original image.

After chaotic permutation and double diffusion, the data is further encrypted using AES-256-GCM:

$$C = AES - GCM(C^{(2)}, K_{AES}, nonce) \quad (14)$$

GCM mode provides not only confidentiality but also data integrity. The original paper emphasizes that the combination of chaotic transformations and AES-GCM allows for the unification of the benefits of chaotic cryptography and standard cryptographic primitives.

The final encrypted file has the following structure:

$$File_{enc} = \{salt, nonce, tag, metadata, C\} \quad (15)$$

Results and discussion. The proposed modified image encryption algorithm is based on a multi-stage data transformation. Its structure includes a global permutation, a block permutation, a first chaotic diffusion, a second diffusion with feedback, and final AES-256-GCM encryption.

The general scheme of the algorithm can be represented as the following stages

$$P \to Perm(P) \to BPerm(P) \to D1(P) \to D2(P) \to AES - GCM \to C. \quad (16)$$

As a result of global random permutation, the pixels of the original image change their positions according to a sequence formed using the logistic mapping. This leads to the destruction of the image's spatial structure. If neighboring pixels in the original image have similar values and a high correlation, then after permutation this dependence is significantly reduced.

Block permutation enhances this effect by further shuffling elements within individual image fragments. Unlike a standard global permutation, block permutation reduces the likelihood of preserving local statistical dependencies. Since the block size depends on the key material, the shuffling structure becomes unique for each secret key.

The first diffusion modifies pixel values using a pseudo-random byte stream generated using tent mapping. This stage aims to smooth out the distribution of pixel values and eliminate the characteristic features of the original image histogram.

The second feedback diffusion enhances the avalanche effect. Changing one pixel of the original image changes not only the corresponding byte of the intermediate result, but also all subsequent bytes, since each new element depends on the previous encrypted value. This increases the algorithm's resistance to differential cryptanalysis.

A comparison of the basic [1] and modified algorithms was carried out, the results of which are presented in Table 1.

The following metrics were used to evaluate the effectiveness of the proposed algorithm: entropy, adjacent pixel correlation, histogram analysis, NPCR, and UACI. These metrics are also used in [1] to evaluate the robustness of image and binary data encryption.

The entropy of the encrypted image tends to 8 bits per pixel:

$$H = -\sum_{i=0}^{255} p_i \log_2 p_i$$

The closer the entropy value is to 8, the more uniform and random the distribution of pixel values. [1] notes that the entropy of encrypted data approaches the theoretical maximum, indicating a high degree of randomness and the elimination of statistical dependencies.

The correlation coefficient of adjacent pixels is defined as follows:

$$r_{xy} = \frac{cov(x,y)}{\sqrt{D(x)}\sqrt{D(y)}}$$

For the original image, this indicator is usually high, since adjacent pixels are visually and statistically related. After encryption, the correlation coefficient should approach zero. This means that the encrypted image does not preserve the spatial structure of the original image.

Table 1- Comparison of the basic and modified algorithms

Criterion	Basic algorithm [1]	Modified algorithm
Chaotic system	Logistic mapping	Logistics + awning display
Permutation	Global chaotic permutation	Global + block permutation
Diffusion	One stage of XOR diffusion	Double diffusion with feedback
Key generation	Scrypt	Scrypt with extended key material separation
Integrity control	AES-GCM	AES-GCM
Key sensitivity	High	Increased
Avalanche effect	High	Enhanced
Robustness to statistical analysis	High	Increased
Resistance to differential analysis	High	Increased

The NPCR metric shows the proportion of changed pixels in the encrypted image when one pixel of the original image changes:

$$NPCR = \frac{\sum_{i,j} D(i,j)}{M * N} * 100\%, \quad (17)$$

where

$$D(i,j) = \{0, C_1(i,j) = C_2(i,j)$$
$$1, C_1(i,j) \neq C_2(i,j)$$

A high NPCR value indicates that a small change in the original image results in a significant change in the encrypted result.

The UACI metric shows the average intensity of differences between two encrypted images:

$$UACI = \frac{1}{M * N} * \sum_{i,j} \frac{|C_1(i,j) - C_2(i,j)|}{255} * 100\% \quad (18)$$

A high UACI value confirms the presence of a pronounced avalanche effect.

The histogram of the encrypted image should be nearly uniform. If the histogram of the original image has pronounced peaks and patterns, then after encryption, the distribution of pixel values should become uniform. This complicates statistical analysis and recovery of information about the original image.

It should be noted that the proposed algorithm does not replace standard cryptographic primitives, but rather complements them. Chaotic dynamics are used as a pre-mixing and diffusion step, while AES-256-GCM provides a cryptographically verified level of security and data authentication. This hybrid approach is more secure than purely chaotic schemes, which often lack a built-in integrity control mechanism.

Conclusion. The study resulted in the development of a modified image encryption algorithm based on chaotic dynamics, designed to improve the security of digital visual data in modern information and telecommunications systems. The relevance of the proposed approach stems from the fact that images possess specific properties that distinguish them from text and other binary information. These properties include high correlation between adjacent pixels, spatial structure, data redundancy, and large data volumes. Therefore, effective image protection requires not only the use of standard cryptographic algorithms but also the prior destruction of their statistical and visual dependencies.

The study explores a hybrid encryption architecture combining chaotic transformations and AES-256-GCM. This approach is more robust than purely chaotic schemes, as chaotic dynamics ensure data permutation and diffusion, while AES-GCM additionally guarantees confidentiality, integrity, and authentication of the ciphertext. The proposed modification further develops this idea by introducing additional image processing stages.

The main distinguishing feature of the developed algorithm is its use of two chaotic mappings: the logistic mapping and the tent mapping. The logistic mapping is used to generate a global permutation sequence, which redistributes the original image pixels to new positions and destroys the original spatial structure.

The tent mapping is used for block permutation and diffusion flow generation, which enhances local data mixing and increases the complexity of encrypted image analysis.

An additional modification element is key-dependent block permutation. After global shuffling, the image is divided into blocks whose size is determined by the parameters of the key material. Within each block, an additional chaotic permutation is performed. This reduces the likelihood of preserving local statistical dependencies that may arise in monochromatic areas of the image, repeating fragments, or individual color channels. Thus, the algorithm provides a more profound destruction of the image's internal structure.

A distinctive feature of this work is the introduction of double diffusion with feedback. The first diffusion modifies pixel values using a chaotic pseudorandom flow, while the second creates a chain-like dependency between the bytes of the ciphertext. As a result, a change in a single pixel of the original image or a minor change in the secret key affects not only the individual element but also subsequent elements of the encrypted sequence. This mechanism enhances the avalanche effect and improves the algorithm's resistance to diff erential cryptanalysis.

The key material is generated using the Scrypt function, which improves resistance to brute-force attacks and attacks using pre-prepared tables. In the proposed algorithm, the key material is divided into several parts: for AES-256-GCM, logistic mapping parameters, tent mapping parameters, block permutation, and feedback. This division ensures the independence of the encryption stages and increases the algorithm's sensitivity to changes in the secret key.

The scientific novelty of this work lies in the development of a modified algorithm that differs from the scheme [1] by employing two chaotic mappings, a key-dependent block permutation, and a second feedback diffusion. This combination is aimed at more deeply disrupting the spatial and statistical structure of the image, increasing sensitivity to the key, and enhancing the avalanche effect.

The practical significance of this research lies in the fact that the proposed algorithm can be applied to image protection in telecommunications systems, video surveillance systems, medical information systems, biometric services, unmanned platforms, and intelligent monitoring systems. The algorithm can be used as a standalone image protection module or as part of a larger system for secure transmission and storage of multimedia data.

Since the image in the algorithm is represented as a byte sequence, the proposed approach can also be adapted to protect other types of multimedia and binary data.

The proposed modified image encryption algorithm based on chaotic dynamics combines the advantages of chaotic systems and standard cryptographic mechanisms. Chaotic transformations ensure the destruction of spatial and statistical image dependencies, while AES-256-GCM provides reliable authenticated encryption. The introduction of two chaotic mappings, a block permutation, and double feedback diffusion improves the algorithm's robustness compared to a hybrid scheme [1].

Литература

1. Mazakova A.T., Jomartova Sh.A., Yessenbaeva A.L., Kulzhanova A.A., Zhao B. Hybrid Encryption Architecture Based on Chaotic Dynamics and AES-GCM Algorithm for Protecting Multimedia Data // Вестник КазУТБ. – 2026.- №2(31). - С.100-111. DOI 10.58805/kazutb.v.2.31-1722.
2. Shannon C.E. Communication Theory of Secrecy Systems //Bell System Technical Journal. - 1949, Vol. 28(4) - P. 656-715.

3. Li Sh., Mou X., Cai Y., Ji Zh., Zhang J. On the security of a chaotic encryption scheme: problems with computerized chaos in finite computing precision // Computer Physics Communications. - 2003.- Vol.153(1) - P.52-58. DOI 10.1016/S0010-4655(02)00875-5.
4. Fridrich J. Symmetric Ciphers Based on Two-Dimensional Chaotic Maps \//International Journal of Bifurcation and Chaos. −1998.-Vol.8 (6). - P.1259-1284. DOI 10.1142/ S021812749800098X.
5. Alvarez G., Li S. Some Basic Cryptographic Requirements for Chaos-Based Cryptosystems // International Journal of Bifurcation and Chaos. −2006.-Vol.16(8). -P.2129-2151. DOI 10.1142/S021812740601597.
6. Wang X., Liu L., Zhang Y. A Novel Chaotic Block Image Encryption Algorithm Based on Dynamic Random Growth Technique // Optics and Lasers in Engineering. −2015.-Vol.66.-P. 10-18. DOI 10.1016/ j.optlaseng.2014.08.005.
7. Pareek N.K., Patidar V., Sud K.K. Image Encryption Using Chaotic Logistic Map // Image and Vision Computing. – 2006, Vol. 24. (9). – P. 926-934. DOI 10.1016/ j. imavis.2006.02.021.
8. Chen G., Mao Y., Chui C.K. A Symmetric Image Encryption Scheme Based on 3D Chaotic Cat Maps//Chaos, Solitons & Fractals. - 2004.-Vol. 21(3). - P.749-761. DOI 10.1016/j.chaos.2003.12.022.
9. NIST. Advanced Encryption Standard (AES). FIPS PUB 197. National Institute of Standards and Technology. Published November 26, 2001; Updated May 9, 2023. DOI 10.6028/NIST.FIPS.197-upd1
10. Dworkin M. Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC. NIST Special Publication 800-38D. 2007. DOI 10.6028/NIST.SP.800-38D.
11. Swati K., Hitesh T. Implementation of Privacy-Preserving Identifiers for the Secure Storage of Electronic Health Records on the Ethereum Blockchain // Distrib. Ledger Technol. - 2026.- Vol.5(2). - P.1-25. DOI 10.1145/3743695.
12. Strogatz S.H. Nonlinear Dynamics and Chaos: With Applications to Physics, Biology, Chemistry, and Engineering. - Westview Press, 2015. - 513 p. ISBN 13: 978-0-8133-4910-7 (pbk).

Сведения об авторах

Мазақова Ә. Т. - PhD, старший преподаватель, Казахский национальный университет им. аль-Фараби, Алматы, Казахстан, e-mail: aigerym97@mail.ru;

Джомартова Ш.А.- доктор технических наук, профессор, Казахский национальный университет им. аль-Фараби, Казахстан, Алматы, e-mail: jomartova@mail.ru;

Есенбаева А.Л.- докторант, Евразийский национальный университет им. Л.Н. Гумилева, Астана, e-mail: Yessenbaeva@mail.ru;

Майлыбаева А.Д. - кандидат физико-математических наук, доцент, Атырауский университет им. Х. Досмухамедова, Атырау, Казахстан, e-mail: a.maylibayeva@asu.edu.kz;

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

Information about the authors

Mazakova A.- PhD, senior lecturer, Al-Farabi Kazakh National University, Almaty, Kazakhstan, e-mail: aigerym97@mail.ru;

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

Yessenbaeva A.- doctoral student, L.N.Gumilyov Eurasian National University, Astana, Kazakhstan, e-mail: Yessenbaeva@mail.ru;

Mailybayeva A. - PhD, Associate Professor, Kh. Dosmukhambetov Atyrau University, Atyrau, Kazakhstan, e-mail: a.maylibayeva@asu.edu.kz;

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