DOI: https://doi.org/10.15276/hait.09.2026.01
UDC 00.056

A modified image encryption algorithm based on the chaotic Tent map

Dmitro V. Dmitrishin[1)]
ORCID: https://orcid.org/0000-0002-2291-2364; dmitrishin@op.edu.ua. Scopus Author ID: 55756757000
Vitaly M. Khamitov[1)]
ORCID: https:///orcid.org/0009-0001-3045-8245; hamitov@op.edu.ua. Scopus Author ID: 58309128700
Svitlana G. Antoshchuk[1)]
ORCID: https://orcid.org/0000-0002-9346-145X; asg@op.edu.ua. Scopus Author ID: 8393582500
Viktor O. Boltenkov[1)]
ORCID: https://orcid.org/0000-0003-3366-974X; vaboltenkov@gmail.com. Scopus Author ID: 57203623617
[1)] Odesa Polytechnic National University, 1, Shevchenko Aveю Odesa, 65044, Ukraine

ABSTRACT

In a number of professional image exchange industries over open communication channels, ensuring the confidentiality and security of images is a key requirement. Furthermore, image exchange must be carried out quickly. These industries include telemedicine, forensic and forensic examinations, high-resolution satellite imagery transmission, and the Internet of Things. In this context, developing image encryption algorithms that meet these requirements is highly relevant. Encryption systems based on chaotic maps offer promising solutions for such problems. Chaotic map-based encryption is a data security algorithm (most often, images) that exploits the properties of deterministic chaos to generate pseudorandom sequences. The key advantages of these algorithms are sensitivity to initial conditions; speed—the algorithms are mathematically simple and faster than many classical ciphers; and security—they provide protection against statistical attacks and brute-force attacks thanks to a huge key space. These algorithms are used to encrypt multimedia (particularly images) in industries where high-speed processing of large volumes of data while maintaining a high level of confidentiality is essential. A modified image encryption algorithm based on the Tent chaotic map has been developed. This algorithm generates a long pseudorandom sequence based on a short key (seed). This sequence is then applied to image encryption using the Vernam algorithm. The sequence can be long enough to encrypt a large image. An integrated encryption quality criterion has been developed for comparative evaluation of encryption quality. The integral criterion combines encryption quality metrics (correlation, entropy, and resistance metrics) into a convolution constructed using the ideal point method. To evaluate the quality of the developed encryption algorithm, a preliminary computer experiment was conducted. In the experiment, the developed algorithm was compared with well-known stream and block encryption standards. The experiment revealed that, by most individual criteria and by the integral quality criterion, the developed algorithm is virtually equal to the standards, but operates significantly faster. This allows us to recommend the developed algorithm for real-time image encryption. A limitation of the developed algorithm is its inability to work with compressed images.

Keywords: image encryption; deterministic chaos; chaotic Tent map; Vernam cipher; integrated quality indicator

***For citation*: Dmitrishin D. V., Khamitov V. M., Antoshchuk S. G., Boltenkov V. O. “A modified image encryption algorithm based on the chaotic Tent map”. *Herald of Advanced of Information Technology.* 2026; Vol.9 No.1: 9–19. DOI: https://doi.org/10.15276/hait.09.2026.01**

INTRODUCTION

Global media file traffic covers a wide range of data associated with the transmission and consumption of various media types, such as video, audio, images, and other content formats. If we exclude the entertainment, consumer, and news segments, the remaining professional media traffic segment is dominated by image exchange. Furthermore, professional images transmitted over open communication channels are typically subject to confidentiality and integrity requirements. These requirements are met by image encryption. Furthermore, image exchange in most areas of the professional segment is required to be efficient. This means that the encryption procedures used to protect images must be sufficiently fast. Encryption procedures based on chaotic maps largely satisfy the requirements for efficient and efficient image encryption. In recent years, the number of publications on chaotic image encryption has grown rapidly [1], [2]. This article is devoted to research in this relevant area.

ANALYSIS OF CHAOTIC IMAGE ENCRYPTION METHODS

A number of professional image exchanges over open communication channels require the confidentiality and security of transmitted images. Image encryption in telemedicine is an important aspect of ensuring the confidentiality and security of medical data. The transmitted images here can include computed tomography (CT), magnetic resonance imaging (MRI), ultrasound, fluorography, etc. [3]. Image encryption is an important tool in forensic examination, which helps to quickly transfer and preserve digital evidence. This also includes the rapid exchange of digital evidence and biometric characteristics of suspects and wanted persons [4]. High-resolution satellite imagery is used in various fields, including agriculture, urban planning, environmental monitoring, military operations, and security. Such images may contain important information that can be used for both legal and illegal purposes and are usually also subject to encryption [5]. Image digitization in the context of the Internet of Things is critical to ensuring data security. The Internet of Things (IoT) offers a wide range of image types that can be encrypted before transmission to ensure security and privacy. These include images from video cameras, drones, and IoT sensors in industrial facilities and smart cities [6], [7], [8].

Cryptographic methods are used to solve image encryption problems. Modern cryptography distinguishes between block and stream ciphers. A stream cipher converts a stream of text characters into a stream of ciphertext, with the conversion dependent on the state of the system [9-10].

Stream encryption schemes can be considered from the point of view of nonlinear dynamics. A distinctive feature of these schemes is the embedding of values of a certain selected trajectory of a discrete dynamic system, i.e., constructed with certain given system parameters and a given initial value. In a similar way, a sequence of decimal digits or a bit sequence can be obtained. This sequence is then used as a key to transform the original sequence (the original message) into an encrypted one (ciphertext). The process is carried out by linear operations modulo (two or ten) the elements of the original and key sequences. The simplest stream encryption scheme is the Vernam cipher [10]. A chain encryption scheme is considered secure if the key sequence is truly random and its length is equal to the length of the original message [10]. However, in practice, pseudo-random (pseudo-chaotic) sequences generated by some deterministic generator from a short key (seed) using a discrete dynamic system are used [11], [12], [13], [14]. Despite numerous studies devoted to increasing the cryptographic strength of encryption methods based on nonlinear dynamics methods, a significant drawback of the latter remains their dependence on hardware and software.

The main computational challenge stems from the fact that computers store numbers in registers and memory cells with a limited number of digits, making the system of real numbers represented in the computer discrete and finite. Another problem can arise when the orbit of a dynamic map becomes looped and the cycle length is sufficiently small. In this case, using a key sequence is impossible. A further challenge arises from the fact that different platforms (hardware and software) use different algorithms for calculating mathematical functions and store intermediate results with varying precision. Since chaotic generators are extremely sensitive to precision, it is highly likely that the same encryption algorithms implemented on different platforms will produce different results.

Thus, the property of chaos in dynamic systems turns out to be dual: on the one hand, it provides the properties of diffusion and confusion (relative to the text and the key) that are absolutely necessary for cryptography [15], [16], [17], on the other hand, it causes inconveniences in use associated with strong sensitivity to disturbances and roundings.

The analysis shows that existing problems can be addressed to some extent by developing methods for generating long pseudo-chaotic sequences using new discrete dynamic systems. In this case, the system parameters and initial values should be used as a seed (short key). Seed requirements: the seed should consist of a small number of elements. Algorithm requirements: the algorithm should be independent of hardware and software.

THE PURPOSE AND OBJECTIVES OF THE WORK

The aim of the work is to develop and conduct preliminary experimental testing of a modified image encryption algorithm based on the chaotic reflection Tent.

To achieve the goal, the following tasks were solved:

– development of a modified image encryption algorithm

– formation of an integral indicator of image encryption quality

– preliminary experimental verification of the developed algorithm and comparative assessment of its quality.

DEVELOPMENT OF A MODIFIED IMAGE ENCRYPTION ALGORITHM

Consider a nonlinear equation with discrete time:

$$x_{n+1} = f(\ x_n),\ \ n = 1,\, 2, \dots\ , \qquad (1)$$

where

$$f(x) = H(1/2 - |x - 1/2|) = \begin{cases} H\,x, x \le 1/2 \\ H(1-x), x > 1/2 \end{cases}, \qquad (2)$$

$x \in (-\infty, +\infty)$, $H \ge 2$. Map (2) is called the generalized Tent map.

A set $\{\eta_1, \dots , \eta_T\}$is called T a cycle of the map (2) if the numbers $\eta_1, \dots , \eta_T$ are different and $\eta_{j+1} = f(\eta_j)$, $j = 1, \dots, T-1$, $\eta_1 = f(\eta_T)$, and each point T of the cycle is called T a periodic point. The multiplier of a cycle of equation (1) is defined by the formula $\mu = f'(\eta_T) \cdot \ldots \cdot f'(\eta_1)$, $\mu = \pm H^T$ i.e. Since $|\mu| = H^T > 1$, any cycle of equation (1) is unstable.

Along with equation (1), let us consider the equation

$$x_{n+1} = F(\ x_n),\ \ n = 1,\, 2, \dots\ , \qquad (3)$$

where $F(x) = f(\ \vartheta x + (1-\vartheta)\, f^{(T)}(x))$, ϑ is some real number called the control parameter and subject to further determination.

We will call equation (3) the control system for equation (1).

Let be a cycle $\{\eta_1, \dots , \eta_T\}$of equation (1). Since $\vartheta \eta_k + (1-\vartheta)\, f^{(T)}(\eta_k) = \eta_k$, this $F(\eta_k) = f(\eta_k)$means that a cycle of equation (1) will also be a cycle of equation (3). It should be noted that the converse statement is generally not true. The multiplier of λ this same cycle $\{\eta_1, \dots , \eta_T\}$ for equation (3) can be found from the expression: $\lambda = \mu(\vartheta + (1-\vartheta)\,\mu)^T$.

Then the condition of local asymptotic stability of the cycle of equation (3) for $\mu = H^T$: $|\lambda| = \left| H^T\,(\vartheta + (1-\vartheta)\,H^T)^T \right| < 1$, whence

$$\frac{H^T - \frac{1}{H}}{H^T - 1} < \vartheta < \frac{H^T + \frac{1}{H}}{H^T - 1}. \qquad (4)$$

If $\mu = -H^T$ the condition of local asymptotic stability of the cycle of equation (5): $|\lambda| = \left| H^T\,(\vartheta - (1-\vartheta)\,H^T)^T \right| < 1$, whence

$$\frac{H^T - \frac{1}{H}}{H^T + 1} < \vartheta < \frac{H^T + \frac{1}{H}}{H^T + 1}. \qquad (5)$$

The following theorem can be proven: if inequalities (4) and (5) are satisfied, then any solution to equation (3) is bounded. Moreover, any T cycle $\{\eta_1, \dots , \eta_T\}$of this equation for which the value $\mu = f'(\eta_T) \cdot \ldots \cdot f'(\eta_1)$is positive/negative is locally asymptotically stable.

To generate a pseudostochastic sequence, we propose using the dynamic system (3), in which ϑ satisfies condition (4) or (5). The sequence itself is defined through T- periodic points $\{\eta_1, \dots , \eta_T\}$. Here, T is a sufficiently large number. To exclude short subcycles, the number T should be taken as prime. There are a total $\frac{2^{T-1} - 1}{T}$of cycles of length T , i.e., there are a great many large T cycles, so the probability of hitting a specific cycle is very small. Due to the chaotic nature of the dynamic system (1), a long cycle is practically indistinguishable from an arbitrary non-cyclic trajectory. This cycle depends on the starting point $x_0 \in (0,1)$, on the number T and the parameters H and ϑ. This effectively makes the cycle uncomputable for cyberattacks. This cycle is locally asymptotically stable. This means that the resulting trajectory does not depend on minor perturbations, computational errors and rounding. Moreover, one can expect that for the same values of x_0 , T , H, ϑ the same cycles will be obtained on different computers. An important issue is the accuracy of the calculations. In general, this accuracy should depend on the cycle length. Computational experiments show that the bit depth also needs to be chosen. $Digits = T + 2(k_1 + k_2)$, $k_1, k_2 \approx 10 - 15$, $k_1 < k_2$. In this case, all significant digits of the numbers can be used η_j to construct key pseudo-chaotic sequences (to enhance the randomness, digits from position k_1 up to can be used $T + k_1 - 1$). There can be multiple starting points. Sequences can be generated by varying the parameters T , H and ϑ.

Practical recommendations for selecting the control parameter:

$$\vartheta = \frac{H^T - \alpha_1 \frac{1}{H}}{H^T + 1} \text{ or } \vartheta = \frac{H^T + \alpha_2 \frac{1}{H}}{H^T - 1},$$
$$(0 < \alpha_1 < 0.001,\ 0 < \alpha_2 < 0.001).$$

The randomness of the key sequence can be further increased: first, select all numbers from the sequence $\{x_j\}_{j=T_0}^{T_0+T}$ (T_0 is a given number) that are in k_1 the place after the decimal point in each x_j, then select the numbers in $k_1+1$the place in the same way, and so on. The generated sequence contains pT^2 elements, where p is the number of starting points. The seed of generation is the key $Key=[T, H, \alpha_1, \alpha_2, \{x_0\}]$, where $\{x_0\}$is the set of starting points. If the parameters $H, \alpha_1, \alpha_2, \{x_0\}$ are determined m by numbers, then there are more possible sequence variants $10^{(3+p)m}$. Such a key sequence space cannot be cracked by brute force.

The procedure for encrypting an image based on the proposed generation of a pseudo-random sequence is as follows:

– a short key is generated $Key=[T, H, \alpha_1, \alpha_2, \{x_0\}]$. The key is stored on the transmitting side and transmitted to the receiving side;

– an image with a height h of pixels and a width w of pixels consists of $n=h\cdot w$pixels, i.e., it is considered an array of n elements, each of which is assigned a three-dimensional vector of decimal numbers. These numbers have 15 digits and are contained between zero and one. The vector (0, 0, 0) defines a black pixel, and the vector (1, 1, 1) defines a white pixel. The coordinates characterize the shades of red, green, and blue, respectively. Sometimes a fourth coordinate is considered, which characterizes the transparency of the color. To encrypt an image based on a short key, it is necessary to generate a pseudo-chaotic sequence whose elements are contained between zero and one, and add it elementwise modulo 2 with the sequences R, G and B. This is the well-known Vernam cipher (or XOR cipher). Instead of one pseudo-chaotic sequence, three different similar sequences can be generated.

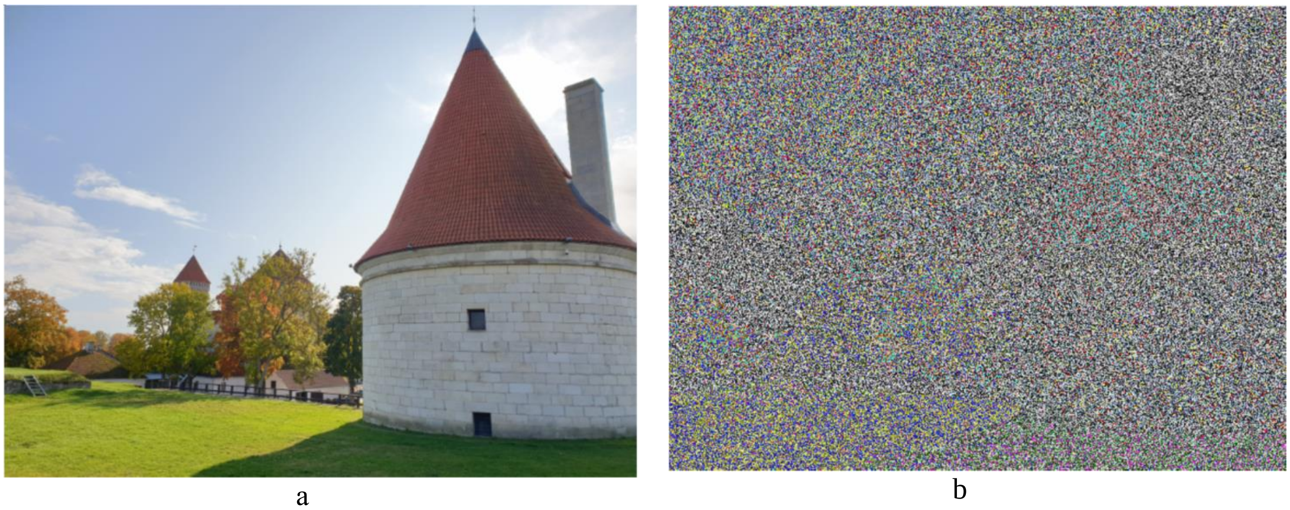
The encrypted image is transmitted to the receiving end. On the receiving end, a similar pseudorandom sequence is generated based on the short key, and the encrypted image is also expanded using the XOR operation.

Let's consider the image shown in Figure 1a as an example. It contains 238,572 pixels ($h=423$, $w=564$). For encryption, we'll take the key $Key=[223,\ 2.070811,\ 0.001,\ 0.9]$and generate a key sequence. It contains 49,729 elements. Additional sequences need to be generated. We'll do this by choosing keys $Key_j=[223,\ 2.07081j,\ 0.001,\ 0.9]$, $j=2,...,6$. The combined key sequence contains elements, which is sufficient to complete the encryption process. The image encrypted in this way is shown in Fig. 1.

FORMATION OF AN INTEGRAL INDICATOR OF IMAGE ENCRYPTION QUALITY

To compare the quality of encryption using the proposed method based on known quality metrics, it is necessary to form an integral quality metric.

Image encryption quality metrics allow you to assess how effectively and securely an image has been encrypted. Various metrics are discussed below.



a b

Fig. 1. **An example of image encryption using the described method a – original; b – encrypted images**

Source: **compiled by the authors**

Correlation

A high-quality encryption algorithm should minimize the correlation between adjacent pixels. The correlation coefficient indicates the linear relationship between adjacent pixels. For effective encryption, it should be close to zero [19].

The correlation coefficient is calculated using the following ratios:

$$\begin{cases} r_{xy} = \dfrac{\operatorname{cov}(x,y)}{\sqrt{D(x)D(y)}}, \\ \operatorname{cov}(x,y) = E([x-E(x)][y-E(y)]), \\ E(x) = \dfrac{1}{N}\sum\limits_{i=1}^{N} x_i, \\ E(y) = \dfrac{1}{N}\sum\limits_{i=1}^{N} y_i, \\ D(x) = \dfrac{1}{N}\sum\limits_{i=1}^{N}[x_i - E(x)], \\ D(y) = \dfrac{1}{N}\sum\limits_{i=1}^{N}[y_i - E(y)], \end{cases} \quad (6)$$

where *x* and *y* are a pair of adjacent pixels, *E*(*x*) and *E*(*y*) is the mathematical expectation of the pixel intensity, *D*(*x*) and *D*(y) is the variance of the intensity.

To account for the correlation between adjacent pixels, the correlation coefficient must be estimated for all possible geometric arrangements of adjacent pixels: horizontal – r_{xy}^{horiz}, vertical – r_{xy}^{vert}, diagonal – r_{xy}^{diag}, anti-diagonal – r_{xy}^{diag}. To estimate the weakest direction of correlation suppression of the original image pixels, it is proposed to calculate the maximum correlation coefficient.

$$r_{xy}^{\max} = \max\left\{r_{xy}^{horiz} + r_{xy}^{vert} + r_{xy}^{diag} + r_{xy}^{antidiag}\right\}. \quad (7)$$

Information entropy of an encrypted image

The information entropy of the encrypted image *C* is calculated as:

$$H(C) = \sum_{i=0}^{2^N-1} p(m_i)\log\frac{1}{p(m_i)}(bit), \quad (8)$$

N is the number of different pixel values (*N* = 256 for an 8-bit image). For an ideal cipher, *H*(*C*)=8 bits.

Local entropy [20]

A more accurate measure of the randomness of an encrypted image is the entropy calculated from local image blocks. Even if an encrypted image has very high Shannon entropy across the entire image, the image may contain some blocks with low entropy. In this sense, it is not perfectly encrypted, no matter how high its global entropy.

Local entropy is calculated using the relation

$$\overline{H(C)} = \sum_{i=1}^{k}\frac{H(S_k)}{k}(bit), \quad (9)$$

where $S_1, S_2, ..., S_k$ are randomly selected non-overlapping k image blocks with T_B pixels each located inside the encrypted image. Calculated $H(S_k)$ $i \in \{1,2,...,k\}$ by the relation () and is further estimated $\overline{H(C)}$. For an ideal cipher, $\overline{H(C)}$ it is also 8 bits.

Attack Resistance Metrics [21]

Number of Pixels Change Rate *(NPCR)* metric is used to evaluate the avalanche effect of an encryption algorithm. It measures how much the encrypted image changes after encryption when a single pixel in the original image is changed. An encrypted image is generated according to the encryption algorithm $C^{(1)}$. Then, a single pixel is changed in the original image, and an encrypted image is generated for the changed image $C^{(2)}$. *NPCR* is calculated as

$$NPCR = \frac{1}{N}\sum_{i=1}^{N}\left(\frac{C^{(1)} \otimes C^{(2)}}{255}\right)\cdot 100\%, \quad (10)$$

where *N* is the number of pixels in the image, $\otimes$ is XOR operation.

NPCR shows what proportion of pixels changed when one bit was changed in the original image. The theoretical ideal value *NPCR* 99.6 %.

UACI (Unified Average Changing Intensity) metric is used to evaluate the quality of image encryption by measuring how much the pixel intensity changes when a single pixel in the original image is changed.

UACI is calculated using the ratio:

$$UACI = \frac{1}{N}\sum_{i=1}^{N}\left(\frac{C^{(1)} - C^{(2)}}{255}\right)\cdot 100\%. \quad (11)$$

The theoretical ideal *UACI value* is 33.4 % (assuming that pixel intensity $C^{(1)}$ is $C^{(2)}$ uniformly distributed).

Integrated quality indicator

For a comprehensive assessment of the quality of image encryption, the following system of quality criteria is proposed, based on the listed metrics:

$$\begin{cases} Crit_1 = r_{xy}^{\max} \\ Crit_2 = H(C) \\ Crit_3 = \overline{H(C)} \\ Crit_4 = NPCR \\ Crit_5 = UACI \end{cases} . \qquad (12)$$

When comparing the quality of a cipher with other known encryption algorithms, a multi-criteria system is difficult to use to decide on the superiority of one option or another. It is proposed to form an integrated encryption quality indicator based on a set of criteria (12). This is accomplished by forming a convolution of the criteria. To form the convolution, the distance from the ideal point method was used [22]. An ideal point is a vector of criterion values in which each of the *n* criteria achieves its best value $Crit_i^{ideal\_point}, i = \overline{1,n}$.

Then the integrated quality indicator *IntQI*

$$IntQI = \left(\sum_{i=1}^{n} \lambda_i^p (Crit_i - Crit_i^{ideal\_point})^p \right)^{\frac{1}{p}}, \qquad (13)$$

where $\lambda_i, i = \overline{1,n}$ are the normalizing (weighting) coefficients, *p* is a natural exponent.

L $_2$ norm to (13) we have

$$IntQI = \sqrt{\sum_{i=1}^{5} \lambda_i^2 (Crit_i - Crit_i^{ideal\_point})^2} . \qquad (14)$$

EXPERIMENTAL EVALUATION OF THE QUALITY OF THE DEVELOPED ENCRYPTION ALGORITHM

To evaluate the quality of the developed Modified Tent Cipher (MTC) encryption algorithm, the following preliminary experiment was conducted. The experiment was run on a Win10 (64-bit) platform with an Intel Core i7-9750H processor running at 2.60 GHz and 8 GB of RAM.

Twenty images of 564×423 pixels in size were encrypted with the MTC cipher, the mordern Ukrainian stream cipher DSTU 8845:2019 “Strumok” with a 256-bit key [23] and the AES block cipher with a 256-bit key in the ECB mode [24]. The above-mentioned quality criteria and were calculated for all encrypted images *IntQI*. The averaged indicators for the 20 images are given in the table 1 An example of image encryption using the MTC cipher is shown in Fig. 2. For this example *Crit*$_1$=0.0018, *Crit*$_2$=7.9970, *Crit*$_3$=7.9022, *Crit*$_4$=98.76, *Crit*$_5$=33.10, *IntQI*=34.15. Encrypted with Strumok-256 AES-256 ciphers the image Fig.2a are visually practically indistinguishable from Fig. 2b , and the quality indicators differ by no more than 5%.

Images encrypted with the Strumok-256 AES-256 ciphers are visually indistinguishable from Fig. 2b. When calculating the local entropy, $\overline{H(C)}$ *k* = 16 blocks of 32 ×32 pixels in size were randomly selected from the encrypted images.

In addition, the encryption/decryption time was recorded for each encryption algorithm.

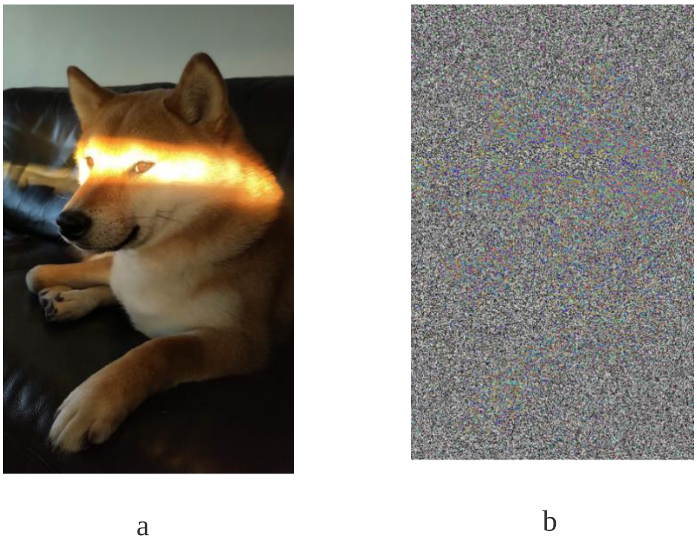


Fig. 2. **Example of the original and encrypted Modified Tent Cipher images: a – original image ; b – encrypted image**

Source: **compiled by the authors**

Based on experience in modeling encryption systems, the following values of the normalizing coefficients were adopted: $\lambda_1 = 10^{4}$, $\lambda_2 = 10^{5}$ bit $^{-1}$, $\lambda_3 = 10^{4}$ bit $^{-1}$, $\lambda_4 = 10^{2}$, $\lambda_5 = 10^{2}$. With these values of the normalizing coefficients, the values *IntQI* for most encryption systems are 25...50. Note that when calculating the *IntQI*, *NPCR* and *UACI* criteria , they are taken not as a percentage, but as a decimal fraction. The results of calculating the partial criteria and the integral quality indicator for encryption with various ciphers are presented in Table 1. The average encryption/decryption time of one image for each encryption algorithm is shown in the Table 2.

Table 1. **Encryption quality criteria**

Quality criteria	MTC	Strumok-256	AES-256
$Crit_1 = r_{xy}^{\max}$	0,0021	0,0019	0,0019
$Crit_2 = H(C)$	7.99961	7.99984	7.99990
$Crit_3 = \overline{H(C)}$	7.9018	7.9123	7.9031
$Crit_4 = NPCR$	98.87	98.91	98.93
$Crit_5 = UACI$	33.18	33.27	33.29
IntQI	33.88	31.02	30.43

Source: **compiled by the authors**

Graphically, comparative indicators of the quality and performance of the ciphers are shown in Fig. 3.

Table 2. **Average encryption/decryption time for one image**

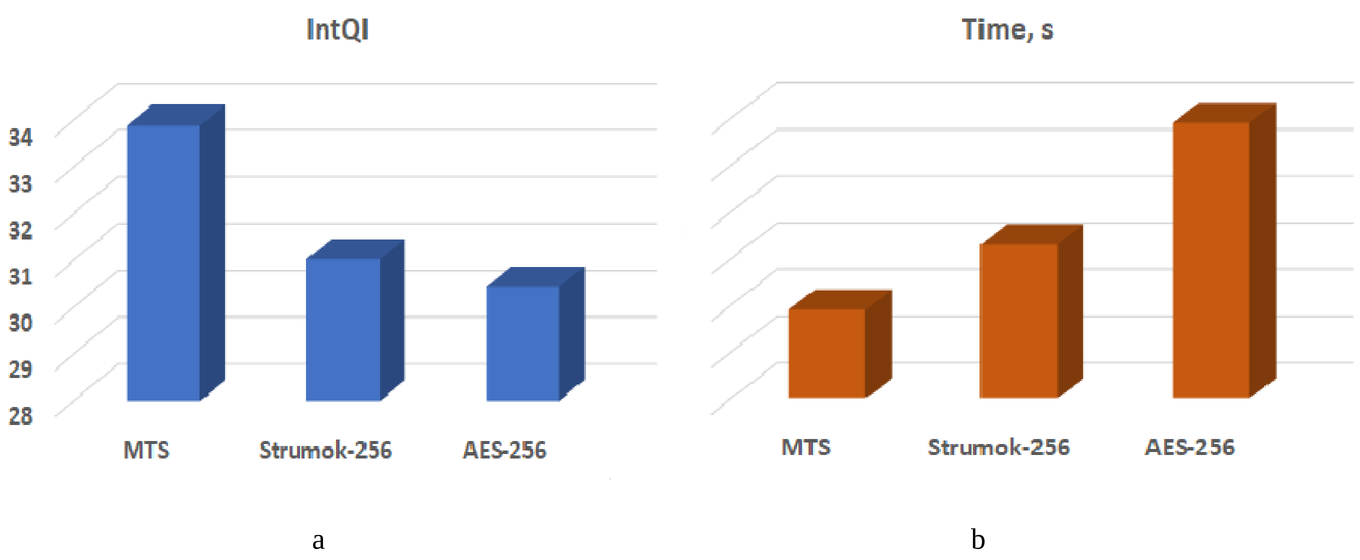
Cipher	MTC	Strumok-256	AES-256
Time, s	0.19	0.34	0.59

Source: **compiled by the authors**

DISCUSSION RESULTS

A preliminary experiment showed that the developed MTS encryption algorithm is almost as good as modern stream and block encryption standards in terms of its integral quality indicator. At the same time, the developed algorithm is significantly faster (almost twice as fast as DSTU 8845:2019 "Strumok" and three times faster than AES-256). This is crucial for the efficiency of professional encrypted image exchange systems. This is explained by several factors. First, the Vernam cipher is based on simple mathematical operations. Second, this cipher combines the scattering and mixing operations, while in standard ciphers they are performed sequentially. Furthermore, the encryption/decryption operations in MTS are identical, while in standard stream and block ciphers they are different.

A drawback of the developed algorithm is its inability to be used with images in compressed formats, such as JPEG. In these formats, the XOR operation during decryption destroys the structure of the compressed [25], [26].



a

b

Fig. 3. **Comparative indicators of quality and performance of ciphers: a – *comparative indicators of quality*; b – average time to encrypt/decrypt one image**

Source: **compiled by the authors**

To fully investigate the proposed algorithm, it is necessary to test the generated pseudorandom sequence using NIST benchmarks, conduct experiments on large, statistically significant samples, and conduct experiments on various hardware platforms. These will be areas for further research.

Nevertheless, preliminary results demonstrate the promise of the developed algorithm.

CONCLUSIONS

1. A modified image encryption algorithm based on the Tent chaotic map was developed. The algorithm generates a long pseudorandom sequence based on a short key (seed). This sequence is then applied to image encryption using the Vernam algorithm.

2. For comparative evaluation of encryption quality, an integral criterion has been formed Encryption quality. The integral criterion combines encryption quality metrics (correlation, entropy, and resistance metrics) into a convolution constructed using the ideal point method.

3. To evaluate the quality of the developed encryption algorithm, a preliminary computer experiment was conducted. In the experiment, the developed algorithm was compared with established stream and block encryption standards. The experiment revealed that, by most individual criteria and the overall quality criterion, the developed algorithm is virtually equal to the standards, but operates significantly faster. This provides grounds for recommending the developed algorithm for real-time image encryption.

Thus, an important theoretical and practical problem of developing and preliminary experimentally testing a modified image encryption algorithm based on the chaotic Tent map was solved.

REFERENCES

1. Abdulhakeem, R. M. & Zebari, N. A. “Chaos-based image encryption techniques: A comprehensive survey”. *Polaris Global Journal of Scholarly Research and Trends*. 2025; 4 (1): 1–11, https://www.scopus.com/pages/publications/105013250805?origin=resultslist. DOI: https://doi.org/10.22219/pgjst.v4n4a220.

2. Dinu, A. & Frunzete, M. “Image encryption using chaotic maps: Development, application, and analysis”. *Mathematics*. 2025; 13 (16): 2588, https://www.scopus.com/pages/publications/105014482675?origin=resultslist. DOI: https://doi.org/10.3390/math13162588.

3. Ahmed, S. T., Hammood, D. A., Chisab, R. F., Al-Naji, A. & Chahl, J. “Medical Image Encryption: A Comprehensive Review”. *Computers*, 2023; 12 (8): 160, https://www.scopus.com/pages/publications/85169018029?origin=resultslist. DOI: https://doi.org/10.3390/computers12080160.

4.Yu, Y., Lu, Y., Li, L., Chen, F. & Yan, X. “Image Forensics in the Encrypted Domain”. *Entropy*. 2024; 26 (11): 900, https://www.scopus.com/pages/publications/85210437014?origin=resultslist. DOI: https://doi.org/10.3390/e26110900.

5. Alexan, W., Maher, E. A., Mamdouh, E. et al. “A chaos-based augmented image encryption scheme for satellite images using Fredkin logic”. *Sci Rep*. 2025; 15: 37345, https://www.scopus.com/pages/publications/105019772527?origin=resultslist. DOI: https://doi.org/10.1038/s41598-025-22008-z.

6. Zhong, Y., Lai, Q., Zhu, C. & Qin, M. “A new multi-image encryption scheme for Smart Home IoT integrating hyperchaos and compressive sensing”. *Computer Standards & Interfaces*. 2026; 95: 104051m https://www.scopus.com/pages/publications/105012976707?origin=resultslist. DOI: https://doi.org/10.1016/j.csi.2025.104051.

7. Al-Ghaili, A. M., Parizi, R. M., Alharthi, H. S., Karim, M. D. A. & Buyya, R. “A Review on role of image processing techniques to enhancing security of IoT applications”. *IEEE Access*. 2023; 11: 101924–101948, https://www.scopus.com/pages/publications/85171531039?origin=resultslist. DOI: https://doi.org/10.1109/ACCESS.2023.3312682.

8. Abinaya, K., Narayana, P. S. & Prakash, R. B. “Chaos theory-driven image encryption in IoT ecosystems”. *2025 3rd International Conference on Communication, Security, and Artificial Intelligence (ICCSAI)*. Greater Noida, India. 2025. p. 1580–1585, https://www.scopus.com/pages/publications/105012109879?origin=resultslist. DOI: https://doi.org/10.1109/ICCSAI64074.2025.11064166.

9. Katz, J. & Lindell, Y. “Introduction to modern cryptography”. *Chapman and Hall/CRC*. 2021.

10. Wong, D. “Real-World Cryptography”. *Manning Publ*. 2021.

11. Zhu, C. X. “A novel image encryption scheme based on improved hyperchaotic sequences”. *Opt. Commun*. 2012; 285: 29–37, https://www.scopus.com/pages/publications/105008069201?origin=resultslist. DOI: https://doi.org/10.1016/j.optcom.2011.08.079.

12. Lu, Q., Yu, L., Zhu C. Symmetric Image Encryption Algorithm Based on a New Product Trigonometric Chaotic Map. Symmetry 2022, 14, 373, https://www.scopus.com/pages/publications/85125564655?origin=resultslist. DOI: https://doi.org/10.3390/sym14020373.

13. Zhang W., Zhu, Z. & Yu, H. “A symmetric image encryption algorithm based on a coupled logistic-bernoulli map and cellular automata difusion strategy”. *Entropy*. 2019; 21: 504. DOI: https://doi.org/10.3390/e21050504.

14. Gupta, M., Gupta, K. K., Khosravi, M. R., Shukla, P. K., Kautish, S. & Shankar, A. “An intelligent session key-based hybrid lightweight image encryption algorithm using logistic-tent map and crossover operator for Internet of Multimedia Things”. *Wireless Personal Communications*. 2021: 121: 1857–1878, https://www.scopus.com/pages/publications/85112605177?origin=resultslist.

15. Lozi, R. “Can we trust in numerical computations of chaotic solutions of dynamical systems”. *Topology and Dynamics of Chaos, eds. Letellier, Ch. & Gilmore, R., World Scientific Series in Nonlinear Science Series A*. 2013; 84: 63–98. – Available from: https://hal.science/hal-00682818v1/document.

16. Ayers, K., Dmitrishin, D., Radunskaya, A., Stokolos, A. & Stokolos, K. “Search for invariant sets of the generalized tent map”. *Journal of Difference Equations and Applications, Taylor & Francis Group*. 2023: 29 (9-12): 1156–1183, https://www.scopus.com/pages/publications/85139157421?origin=resultslist. DOI: https://doi.rg/10.48550/arXiv.2111.08904.

17. Dmitrishin, D., Stokolos, A. & Iacob J. “Average predictive control for nonlinear discrete dynamical systems”. *Adv. Syst. Sci. Appl*. 2020; 20 (1): 27–49. DOI: https://doi.org/10.48550/arXiv.1906.02925.

18. The, J. S., Alawida, M. & Sii Y. C. “Implementation and practical problems of chaos-based cryptography”. *Journal of Information Security and Applications*. 2020: 50: 102421. DOI: https://doi.org/10.1016/j.jisa.2019.102421

19. Bhattacharjee, S., Gupta, M. & Chatterjee, B. “Time efficient image encryption-decryption for visible and COVID-19 X-ray images using modified chaos-based logistic map”. A*ppl Biochem Biotechnol*. 2023; 195: 2395–2413, https://www.scopus.com/pages/publications/85138708125?origin=resultslist. DOI: https://doi.org/10.1007/s12010-022-04161-7.

20. Ghouate, N. E., Tahiri, M. A. & Bencherqui, A., et al. “A high-entropy image encryption scheme using optimized chaotic maps with Josephus permutation strategy”. *Sci Rep*. 2025; 15: 29439, https://www.scopus.com/pages/publications/105013027461?origin=resultslist.
DOI: https://doi.org/10.1038/s41598-025-14784-5.

21. Zou, C., Shang, Y., Yang, Y., Zhou, C. & Liu, Y. “A novel image encryption algorithm with anti-tampering attack capability.” *Chaos, Solitons & Fractals*. 2024;189 (Part 1): 115638, https://www.scopus.com/pages/publications/85206612516?origin=resultslist.
DOI: https://doi.org/10.1016/j.chaos.2024.115638.

22. Boltenkov, V., Brunetkin, O., Dobrynin, Y., Maksymova, O., Kuzmenko, V., Gultsov, P., Demydenko, V. & Soloviova, O. “Devising a method for improving the efficiency of artillery shooting based on the Markov model”. *Eastern-European Journal of Enterprise Technologies*. 2021; 6 (3 (114)): 6–17, https://www.scopus.com/pages/publications/85123511164?origin=resultslist.
DOI: https://doi.org/10.15587/1729-4061.2021.245854.

23. Kuznetsov, O., Lutsenko, M. & Ivanenko, D. “Strumok stream cipher: Specification and basic properties”. *2016 Third International Scientific-Practical Conference Problems of Infocommunications Science and Technology (PIC S&T)*. Kharkiv, Ukraine. 2016. p. 59–62. https://www.scopus.com/pages/publications/85018444432?origin=resultslist.
DOI: https://doi.org/10.1109/INFOCOMMST.2016.7905335.

24. AL-Wattar, A. H. “A new approach for the image encryption using AES cipher in ECB mode”. *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*. 2020; 14 (2): 1061–1074. DOI: https://doi.org/10.61841/turcomat.v14i03.14117.

25. Kryvenko, S., Lukin, V., Bondžulić, B. & Stojanović, N. “Compression of noisy grayscale images with compression ratio analysis”. *Advanced Information Systems*. 2025; 9 (2), 68–74, https://www.scopus.com/pages/publications/105005120577?origin=resultslist5. DOI: https://doi.org/10.20998/2522-9052.2025.2.09.

26. Gorokhovatskyi, O. & Yakovleva, O. “Medoids as a packing of ORB image descriptors”. *Advanced Information Systems*. 2024. 8 (2): 5–11, https://www.scopus.com/pages/publications/85196384624?origin=resultslist. DOI: https://doi.org/10.20998/2522-9052.2024.2.01.

Conflicts of Interest: The authors declare that they have no conflict of interest regarding this study, including financial, personal, authorship, or other interests, which could influence the research and its results presented in this article. Authors Svitlana G. Antoshchuk and Viktor O. Boltenkov are members of the Editorial Board of this journal. This role had no influence on the peer review process or editorial decision regarding this manuscript

Received 05.01.2026
Received after revision 13.02.2026
Accepted 19.02.2026

DOI: https://doi.org/10.15276/hait.09.2026.01
УДК 004.056

Модифікований алгоритм шифрування зображень на основі хаотичного відображення Tent

Дмитришин Дмитро Володимирович[1)]
ORCID: https://orcid.org/ 0000-0002-2291-2364; dmitrishin@op.edu.ua Scopus Author ID: 55756757000
Хамітов Віталій Миколайович[1)]
ORCID: https://orcid.org/0009-0001-3045-8245; hamitov@op.edu.ua. Scopus Author ID: 58309128700
Антощук Світлана Григорівна[1)]
ORCID: https://orcid.org/0000-0002-9346-145X; asg@opu.ua. Scopus Author ID: 8393582500
Болтьонков Віктор Олексійович[1)]
ORCID: https:// orcid.org/0000-0003-3366-974X; vaboltenkov@gmail.com. Scopus Author ID: 57203623617

АНОТАЦІЯ

У ряді професійних галузей обміну зображеннями по відкритих каналах зв'язку важливою вимогою є забезпечення конфіденційності та збереження зображень. Крім того, обмін зображеннями має здійснюватися оперативно. До таких галузей належать телемедицина, криміналістичні та судові експертизи, передача супутникових зображень високого дозволу, інтернет речей. У цьому плані дуже актуальне завдання розробки алгоритмів шифрування зображень, що забезпечують виконання цих вимог. Перспективними для вирішення таких завдань є системи шифрування, що ґрунтуються на хаотичних відображеннях. Шифрування на основі хаотичних відображень - це алгоритми захисту даних (найчастіше зображень), що використовують властивості детермінованого хаосу для генерації псевдовипадкових послідовностей. Ключові переваги алгоритмів: чутливість до початкових умов, швидкість-алгоритми математично прості і працюють швидше багатьох класичних шифрів, стійкість-безпечують захист від статистичних атак і повного перебору (brute-force) завдяки величезному простору ключів. Алгорити застосовуються для шифрування мультимедіа (зокрема, зображень) у галузях, де важлива висока швидкість обробки великих обсягів даних за збереження високого рівня конфіденційності. Розроблено модифікований алгоритм шифрування зображень виходячи з хаотичного відображення Tent. Алгоритм дозволяє на підставі короткого ключа (насіння) згенерувати довгу псевдовипадкову послідовність. Далі ця послідовність застосовується до шифрування зображення за алгоритмом Вернама. Послідовність може мати довжину, достатню для шифрування зображення великого розміру. Для порівняльної оцінки якості шифрування сформовано інтегральний критерій якості шифрування. Інтегральний критерій поєднує метрики якості шифрування (кореляційні, ентропійні та метрики резистентності) в пакунок, побудований методом ідеальної точки. Для оцінки якості розробленого алгоритму шифрування було проведено попередній комп'ютерний експеримент. В експерименті розроблений алгоритм порівнювався з відомими стандартами потокового та блочного шифрування. В результаті експерименту встановлено, що як за більшістю приватних критеріїв, так і за інтегральним критерієм якості розроблений алгоритм практично не поступається стандартам, але працює значно швидше. Це дає підстави рекомендувати розроблений алгоритм шифрування зображень у реальному масштабі часу. Обмеженням розробленого алгоритму є неможливість роботи із зображеннями стиснутого формату.

Ключові слова: шифрування зображень; детерміноване хаос; хаотичне відображення Tent; шифр Вернама; інтегральний показник якості

ABOUT THE AUTHORS

Dmitro V. Dmitrishin - Doctor of Engineering Sciences, Professor, Department of Applied Mathematics and Information Technologies. Odesa Polytechnic National University, 1, Shevchenko Ave. Odesa, 65044, Ukraine
ORCID: https://orcid.org/ 0000-0002-2291-2364; dmitrishin@op.edu.ua. Scopus Author ID: 55756757000
***Research field*:** Dynamical systems, Information technology

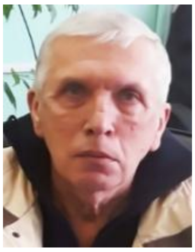
Дмитро Володимирович Дмитришин - доктор технічних наук, професор, кафедра Прикладної математики та інформаційних технологій. Національний університет «Одеська політехніка», пр. Шевченка, 1, Одеса, 65044, Україна

Vitaly M. Khamitov - PhD student, Department of Information Systems. Odesa Polytechnic National University, 1, Shevchenka Ave, Odesa, 65044, Ukraine
ORCID: https://orcid.org/0009-0001-3045-8245; hamitov@op.edu.ua. Scopus Author ID: 58309128700
Research field: Information technology in signal processing

Хамітов Віталій Миколайович - аспірант кафедри Інформаційних систем. Національний університет «Одеська політехніка», пр. Шевченка, 1. Одеса, 65044, Україна

Svitlana G. Antoshchuk - Doctor of Engineering Sciences, Professor, Head of Computer Systems Institute. Odesa Polytechnic National University, 1, Shevchenko Ave. Odesa, 65044, Ukraine
ORCID: https://orcid.org/0000-0002-9346-145X; asg@op.edu.ua. Scopus Author ID: 8393582500
Research field: Pattern recognition; deep learning; object tracking; face recognition; graphic images formation and processing

Антощук Світлана Григорівна - доктор технічних наук, професор, директор Інституту комп’ютерних систем Національний університет «Одеська Політехніка», пр. Шевченка, 1. Одеса, 65044,Україна



Viktor O. Boltenkov - PhD, Associate Professor, Information System Department. Odesa Polytechnic National University, 1, Shevchenko Ave. Odesa, 65044, Ukraine
ORCID: https://orcid.org/0000-0003-2777-3137; vaboltenkov@gmail.com. Scopus Author ID: 57203623617
Research field: Blockchain technologies; signal processing

Болтьонков Віктор Олексійович - кандидат технічних наук, доцент кафедри Інформаційних систем. Національний університет «Одеська політехніка», пр. Шевченка, 1. Одеса, 65044, Україна