DOI: https://doi.org/10.15276/aait.09.2026.14
UDC 004.056.53

A method for operative sharing confidential images among a group of trusted users

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

ABSTRACT

Encryption of high-resolution images plays a key role in ensuring their confidentiality and integrity. Given the rapid growth of traffic of such images in open communication channels, the development of new methods and means of their protection is becoming increasingly **actual**. The **objective** of this study is to develop and model a method for exchanging confidential images for a group of trusted users. In the process of the study, encryption **methods** with chaotic maps, cryptography on elliptic curves, and agreement group secret agreement with various protocols were used . One of the requirements for the method being developed is its operation on a time scale close to real. This is due to the rapid aging of information in images subject to analysis in the group. The study is based on the method of generating a pseudo-random sequence using a modified chaotic map Tent. A short key containing the parameters of this map is transmitted to trusted users who form the group. Then each user can expand the key into a pseudo-random sequence and encrypt/decrypt the image with the Vernam cipher . A group of trusted users is formed using the Diffie-Hellman protocol or Burmester-Desmedt on elliptic curves. The Weierstrass, Montgomery and Edwards curves were analyzed from the point of view of computational costs. The Montgomery curve was chosen as the most computationally efficient working elliptic curve. To transfer to a group of trusted users, the short key of Tent map is encrypted with a block cipher with a secret as the key. The developed method is modeled for the curve Montgomery Curve25519. Image security and confidentiality are ensured by five levels of protection. As a **result**, it was found that group formation according to the Burmester-Desmedt protocol ensures the operation of the method on a time scale close to real time and a high level of scalability.

Keywords: Chaotic Tent map; Vernam cipher; Diffie-Hellman protocol; Burmester-Desmedt protocol; Montgomery elliptic curve

***For citation*: Khamitov V. M., Boltenkov V. O., Antoshchuk S. G. "A method for operative sharing confidential images among a group of trusted users". *Applied Aspects of Information Technology.* 2026; Vol.9 No.2: 200–207. DOI: https://doi.org/10.15276/aait.09.2026.14**

INTRODUCTION

In the professional segment of world media traffic significant place occupy image high permissions. This refers to such areas as satellite transmission images, telemedicine, forensic and forensic examinations, the Internet things [1]. In the majority listed industries images that transmitted over open communication channels, recognized confidential and must to be protected from any malicious interventions [2] . In addition, in the listed industries image are objects quickly aging information That's why additional requirement when transferring such images is functioning of transmission systems in real life or a time scale close to it. Since the need to transfer confidential images constantly growing , the topic of improvement methods of rapid exchange of such images, which dedicated this research quite actual.

© Khamitov V., Boltenkov V., Antoshchuk S., 2026

ANALYSIS OF THE STATE OF THE QUESTION

In recent years , the direction of protecting images by encrypting them using chaotic displays has been intensively developed [3], [4]. Chaotic displays are a powerful tool for encrypting images based on the principles of chaos theory. These methods provide a high level of security due to their unpredictability and complexity [5]. One of the key features of chaotic displays is the ability to generate pseudo-random sequences that can be used to mix image pixels. Unlike traditional encryption methods, such as symmetric and asymmetric encryption, chaotic systems do not require complex mathematical operations, which allow to significantly speeding up the encryption process [6]. The advantage of chaotic methods is also their resistance to attacks, since even small changes in the initial conditions can lead to radically different results. In addition, chaotic maps are easily adapted to different types of images and can be used in real

This is an open access article under the CC BY license (https://creativecommons.org/licenses/by/4.0/deed.uk)

time [7]. Chaotic map Tent for image encryption has a number of unique features that make it attractive for use in cryptography [8]. First, it is characterized by high sensitivity to initial conditions, which provides significant changes in the output data with the smallest changes in the input data. Secondly, Tent map is easily implemented and requires relatively small computing resources, which makes it available for practical use [9]. The combined use of the chaotic tent mapping with the Vernam cipher enhances security, since the Vernam cipher is an ideal cipher that uses a key of the same length as the message [10]. This allows you to additionally mix and mask the data obtained after applying Tent map. However, it is necessary to take into account that the effectiveness of this method depends on the quality of the generation of pseudorandoms sequence in the Tent display. In addition, in order to achieve maximum safety, it is important to correctly choose the parameters of Tent map [11].

THE PURPOSE AND TASKS OF THE WORK

Requirements for the developed method:

1) ensuring the confidentiality and integrity of the images, excluding possible unauthorized interference with the images for the purpose of their modification, copying or viewing;

2) high performance, which ensures functioning in a mode close to real time;

3) the possibility of easy scaling of a group of users.

To achieve the goal of research, the following tasks are solved:

1) development of the algorithmic and functional structure of the method of exchanging confidential images;

2) modeling of the method for confirmation of its functional capabilities and evaluation of the main characteristics.

DEVELOPMENT OF THE ALGORITHMIC AND FUNCTIONAL STRUCTURE OF THE METHOD

The basis of functioning is ensuring confidentiality and security is the modified method of image encryption based on the chaotic map Tent with control described in the paper [12]. This method makes it possible to generate a sufficiently long pseudo-random sequence of high quality. This sequence is then used to encrypt or decrypt the image with the Vernam cipher. The pre-processed image is converted into a vector form. For encryption or decryption, the user must have a long pseudo-random sequence generated by the Tent algorithm. Transmission of such a sequence over open communication channels causes certain difficulties. Therefore, the modified Tent encryption algorithm provides for the formation of a short key containing control parameters for generating a pseudo-random sequence ("seed") $KeyI$. A short session key is generated by an administrator managing the image exchange process in a group of trusted users. This short key is transmitted to users who unfold it into a pseudo-random sequence of the desired length. Image encryption based on chaotic map Tent is the first level of image protection.

At the second level of protection, an approach to forming a group of trusted users and obtaining a common secret is proposed.

Formation of a group of trusted users, and the procedure for obtaining a common shared secret.

The system administrator forms a session group of trusted users who are allowed access to images. Note that users can both encrypt images and display them in a group, and decrypt displayed images for analysis. Because this group of trusted users has a short key of the modified map Tent $KeyI$ transmitted over open communication channels, this key must be encrypted with a block cipher $E_{KeyII}(KeyI)$. Therefore, in the group of users, a common key must be generated $KeyII$ to decrypt the key of the first level. The classic procedure for generating a common agreed key (common secret) is the Diffie-Hellman procedure. The Diffie-Hellman procedure, developed in 1976, originally allowed two users to generate a common secret key. Initially, it was based on one-sided functions of a discrete logarithm or factorization of a product of prime numbers [13]. With the formation of cryptographic procedures on elliptic curves, the Diffie-Hellman procedure was focused on the use of elliptic curves. This made it possible to significantly reduce the size of the keys and, accordingly, the time spent. By the authors it is proposed to form a common secret key for a group of confidential users according to the modified Diffie-Hellman protocol on elliptic curves. To date, more than 10 forms of elliptic curves are known [14]. The three types of electrical curves that are most commonly used are Weierstrass elliptic curves, Montgomery elliptic curves, and Edwards elliptic curves.

To choose the best elliptic curve for the shared secret agreement protocol, the three most commonly used types of elliptic curves are considered: Weierstrass, Montgomery, and Edwards curves.

1. Weierstrass elliptic curves.

Weierstrass elliptic curves are given by the equation:

$$E_w(a,b): y^2 = x^3 + ax + b,$$

where the coefficients a and b belong to the finite field $\mathbb{F}_p$.

2. Elliptic Montgomery curves [15].

Montgomery elliptic curves have the form:

$$E_M(A,B): By^2 = x^3 + Ax^2 + x,$$

where *A* and *B* are parameters belonging to the finite field $\mathbb{F}_p$. These curves are convenient for the implementation of addition and multiplication operations, as they avoid the need to calculate the square root.

3. Elliptic curves of Edwards [16].

Edwards elliptic curves are described by the equation:

$$E_{Ed}(d): x^2 + y^2 = 1 + dx^2y^2,$$

where *d* is a parameter that also belongs to the finite field.

The analysis of three types of curves allows us to state that the Montgomery curve requires the least computational costs for calculations. Addition and multiplication operations on Montgomery curves are performed faster compared to other types of curves. Montgomery curves use an effective algorithm for calculating the multiplication of a point by a scalar - the "Montgomery ladder" [17]. The Montgomery ladder performs operations for a fixed number of steps, regardless of the values of the scalar bits. Therefore, the Montgomery curve is chosen as the basis of the shared secret agreement protocol.

The following protocol is constructed Diffie-Hellman approvals common secret on the elliptical curve Montgomery.

Initial settings of the protocol.

Administrator forms group from *N* confidential users: $U_1, U_2, ..., U_N$, at the same time administrator is a user U_1. Administrator selects and announces general the parameters of the Montgomery elliptic curve are the equation of the curve $By^2 = x^3 + Ax^2 + x$, the finite field $\mathbb{F}_p$, the base point-generator $\mathbf{P}$, and the order of the group *n*. *The following* protocol operations look like this.

1. Key generation: Each user $U_i, i = \overline{1,N}$ chooses a random integer ($x_i (1 < x_i < n-1)$) - this is his private key.

2. Cyclic iterative exchange.

Step 1: U_1 calculates $\mathbf{X_1} = x_1 \cdot \mathbf{P}$ and sends to the user U_2.

Step 2: U_2 receives $\mathbf{X_1}$, calculates $\mathbf{X_2} = x_2 \cdot \mathbf{X_1} = x_2 \cdot (x_1 \cdot \mathbf{P})$ and sends to U_3. …

… *Step i :* The user U_i receives a point $\mathbf{X_{i-1}}$ from U_{i-1}, calculates $\mathbf{X_i} = x_i \cdot \mathbf{X_{i-1}}$ and sends U_{i+1}. …

Step N: The last user U_N receives $\mathbf{X_{N-1}}$ and calculates the last one open point $\mathbf{X_N} = x_N \cdot \mathbf{X_{N-1}} = (x_N x_{N-1} ... x_1) \cdot \mathbf{P}$.

3. Distribution of the secret: The point $\mathbf{X_N}$ is distributed by the administrator to all users.

4. Calculation of the common secret: Every participant U_i receives a point $\mathbf{X_N}$, multiplies it by its secret key and receives a shared secret: $\mathbf{CS} = x_i \cdot \mathbf{X_N}$.

If it is necessary to expand the group of trusted users, that is, to add a new user, the following steps are performed. When a new user U_{new} must join the group, he generates his private key and public key. $\mathbf{P_{new}} = k_{new} \cdot \mathbf{P}$. Existing users transfer their public keys to the new user. The new user also transfers his public key to all existing users. The calculation of the common secret is as follows. Each user calculates a new shared secret using his private key and the public keys of all other participants.

For the user U_i, the shared secret will be calculated as:

$$\mathbf{CS_i} = x_i \cdot \mathbf{P_{new}} + \sum_{j \neq i} x_i \cdot \mathbf{P_j}.$$

An alternative solution at the second level of protection may be the use of the protocol Burmester-Desmedt approvals common secret on the elliptical curve Montgomery [18], which provides next sequence actions:

First stage: Each participant U_i chooses a random number x_i (private key) and publishes his point on the curve: $\mathbf{W_i} = x_i \mathbf{P}$.

Second stage: Each participant calculates and publishes an intermediate value $\mathbf{X_i}$ using the public keys of neighbors:

$$\mathbf{X_i} = (x_i \cdot \mathbf{Z_{i+1}}) - (x_i \cdot \mathbf{Z_{i-1}}),$$

where $\mathbf{Z_{i+1}}$ and $\mathbf{Z_{i-1}}$ are public points of "neighbors" on the right and left in the logical ring of users.

Calculation of the key: After the exchange of values $\mathbf{X_i}$ every participant can calculate the final common secret **CS**. After all the participants U_i have exchanged meanings $\mathbf{X_i}$, each user U_i knows his secret $\mathbf{X_i}$ and received it from $\mathbf{X_j}$ *others*.

Calculates the shared secret key **CS** according to the following formula:

$$\mathbf{CS} = N \cdot x_i \cdot \mathbf{Z}_{i-1} + (N-1) \cdot \mathbf{X}_i + (N-2) \cdot \mathbf{X}_{i+1} + ... + \mathbf{X}_{i+n-2},$$

where N is the total number of participants, x_i is secret key of the current user, $\mathbf{Z}_{i-1}$ is open key of the neighbor on the left, $\mathbf{X}_i$ is values obtained at the second stage.

Note that all indices are calculated modulo N. The main advantage of the Burmester-Desmedt protocol is scalability: the protocol is executed in just two rounds of interaction, regardless of the number of participants.

The third level of protection in the proposed method is the hashing of the shared secret obtained in the Diffie-Hellman protocol:

$$CS' = Hash(CS_x),$$

where *Hash* is a standardized hash function (for example, SHA -3), CS_x is x-coordinate of the point **CS**.

Received meaning CS' is the key with which the short key *KeyI* of the Tent map is encrypted (the fourth level of protection):

$$k = CS',$$

$$KeyII = E_k(KeyI).$$

At the fifth level, the encrypted key *KeyII* is distributed to all users. They can generate a session pseudo-random sequence of Tent map and encrypt/decrypt confidential images of this session.

The structural and logical scheme of the developed method is shown in Fig. 1. As can be seen from Fig. 1 developed method contains 5 levels of protection.

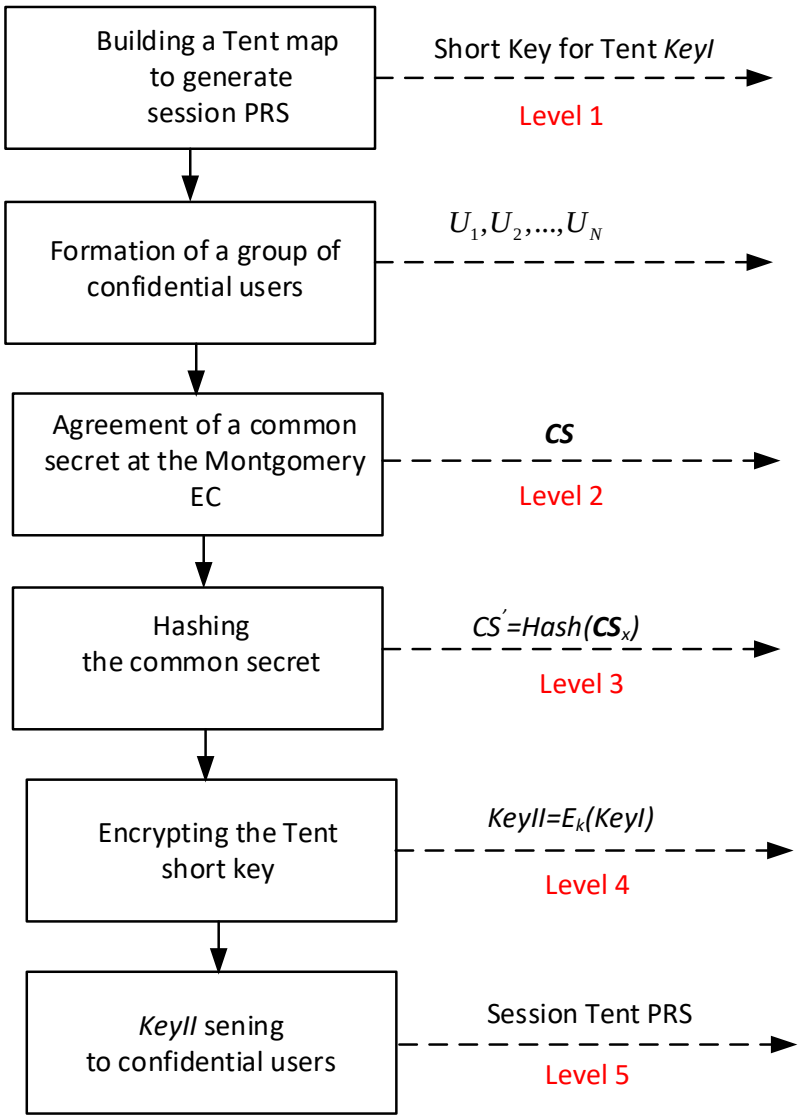

Fig. 1. **Structural and logical scheme of the developed method**

Source: **compiled by the authors**

SIMULATION MODELING OF THE METHOD

Software simulation of the method was carried out on the Win 10 (64-bit) platform with an Intel Core i7-9750H processor with a frequency of 2.60 GHz and 8 GB RAM. A modified map Tent with a set of short keys has been created $KeyI_j = [223, 2.07081j,\ 0.001,\ 0.9]$, $j = 1,...,6$. The group of confidential participants was selected in the composition of N = 5, 10, 20, 30. The Curve25519 curve [19] was chosen as the Montgomery elliptic curve. It was developed by Daniel Bernstein and is one of the most popular elliptic curves for cryptographic applications.

The curve is given by the equation:

$$y^2 = x^3 + 486662x^2 + x.$$

The form of curve shown in Fig. 2.

The curve is defined over a field $\mathbb{F}_p$ with a simple modulus $p = 2^{255} - 19$ (hence its name). Curve Curve25519 is recommended for use NIST thanks to a number of advantages .

– A large order of the group, which is $2^{252} + 27742317777372353535851937790883648493$, made up of a high level of security.

– Fast operations. Algorithms for performing operations on Curve25519 are optimized for speed. This allows you to efficiently perform operations even on devices with limited resources.

– A small number of operations. Calculation of points on a curve requires fewer operations than for other curves, which makes it more productive.

The generator point $G$is selected with coordinates $G = (9, y_G)$. Significance $x_G = 9$ it was chosen because this value is small and simple, which simplifies further calculations.

SHA -3-256 function (Keccak) was used for hashing.

For encryption $KeyII = E_k(KeyI)$ the block cipher standard is applied AES -256. In progress modeling were programmatically implemented both the Diffa-Hellman protocol and the Burmester-Desmedt protocol. The processor time T *was registered* for performing all operations according to the scheme in Fig. 1.

The modeling results are shown in Table 1.

Table 1 demonstrates the high efficiency of the protocol Burmester-Desmedt.

In addition, the data in Table 1 indicate the scaling of the method using this protocol: with the increase in the number of users N e economy processor time compared to application protocol Diffie-Hellman noticeably increases Modeling confirmed the developed method correctness based on algorithmic ones solutions and the operation of the method in a time scale close to the real one.

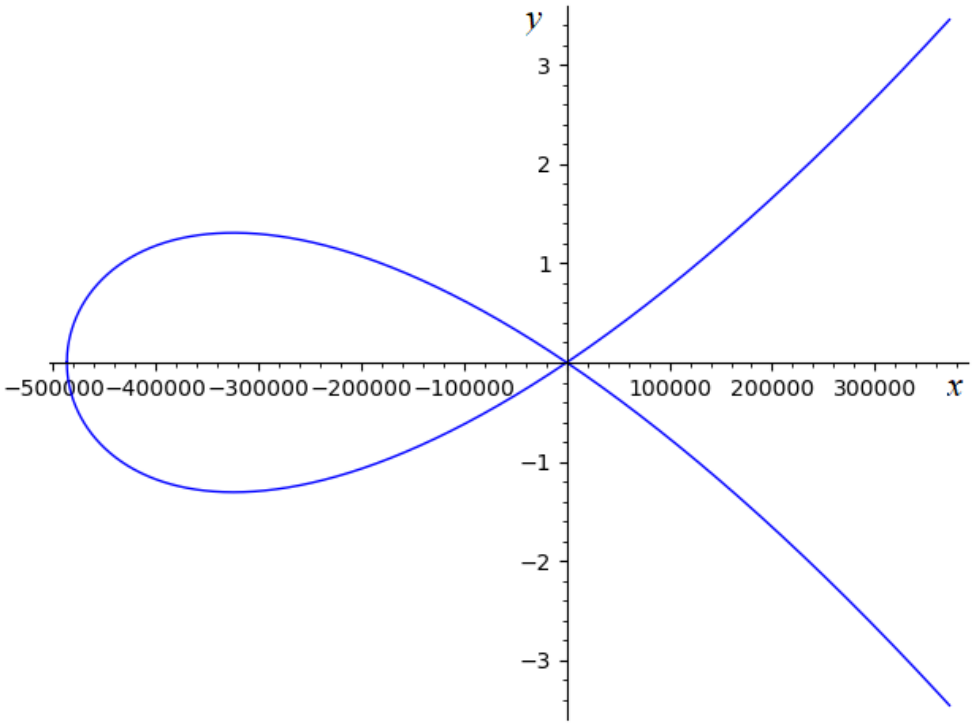

Fig. 2. **The form of Montgomery Curve25519**
Source: **compiled by the authors**

Table 1. **Costs processor time for filling full sequence operations (Fig. 1)**

Number of group members *N*	*T*, s Coordination common secret according to the Diffie-Hellman protocol	*T*, s Coordination common secret according to the Burmester-Desmedt protocol
5	2, 18	0.86
10	3.98	1.23
20	7.34	3.44
30	13.43	5.65

Source: **compiled by the authors**

CONCLUSIONS

A method for operative sharing confidential images among a group of trusted users has been developed. The confidentiality of the images is ensured by the use of encryption with the use of pseudo-random sequences based on the modified chaotic map Tent. In addition, a protocol for forming a group of trusted users, who are allowed access to images, has been developed. Image security is ensured by five levels of protection. The protocol is based on the application of operations on elliptic curves. Simulation modeling of the developed method was carried out. The simulation demonstrated the performance of the method in a time scale close to the real one, and scaling based on the fast Burmester-Desmedt protocol.

REFERENCES

1. Alghamdi, Y. & Munir, A. “Image Encryption Algorithms: A Survey of Design and Evaluation Metrics”. *Journal of Cybersecurity and Privacy.* 2024; 4 (1): 126–152, https://www.scopus.com/pages/publications/85188927822?origin=resultslist. DOI: https://doi.org/10.3390/jcp4010007.

2. Alzoubi S. “Image encryption based on simple shift, permutation and transformation operations on bit layers”. *Data and Metadata*. 2025; 4: 690, https://www.scopus.com/pages/publications/85218798510?origin=resultslist. DOI: https://doi.org/10.56294/dm2025690.

3. Thajeel, N. G. & Mohammed, H. J. “Image Encryption Via Hybrid Chaotic Algorithms”. *Journal of Lifestyle and SDGs Review.* 2026; 6 (1): e08094. DOI: https://doi.org/10.47172/2965-730X.SDGsReview.v6.n01.pe08094.

4. Alexan, W., Shabasy, N. H. E., Ehab, N., et al. “A secure and efficient image encryption scheme based on chaotic systems and nonlinear transformations”. *Sci Rep*. 2025; 15: 31246, https://www.scopus.com/pages/publications/105014427236?origin=resultslist. DOI: https://doi.org/10.1038/s41598-025-15794-z.

5. Zhiqiang, H., Rauf, A., Nazir, A., et al. “Design and analysis of a secure image encryption algorithm using proposed non-linear RN chaotic system and ECC/HKDF key derivation with authentication support”. *Sci Rep*. 2025; 15: 39951, https://www.scopus.com/pages/publications/105021817989?origin=resultslist. DOI: https://doi.org/10.1038/s41598-025-23592-w.

6. Kanwal, S., Inam, S., Shah A. A., et al. “A robust approach to satellite image encryption using chaotic map and circulant matrices”. *Engineering Reports*. 2024; 6 (12): e13010, https://www.scopus.com/pages/publications/85205294678?origin=resultslist.
DOI: https://doi.org/10.1002/eng2.13010.

7. 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.

8. Li, C., Luo, G., Qin, K., et al. “An image encryption scheme based on chaotic tent map”. *Nonlinear Dyn.* 2017; 87: 127–133. DOI: https://doi.org/10.1007/s11071-016-3030-8.

9. Zhou, W., Li, X. & Xin, Z. “Image Encryption Algorithm Based on an Improved Tent Map and Dynamic DNA Coding”. *Entropy*. 2025; 27 (8): 796. DOI: https://doi.org/10.3390/e27080796.

10. Odeh, A., Taleb, A. A., Alhajahjeh, T., et al. “Lightweight secure image encryption: a tent map chaos theory approach”. *Multimed Tools Appl.* 2025; 84: 42379–42398, https://www.scopus.com/pages/publications/105014521762?origin=resultslist. DOI: https://doi.org/10.1007/s11042-025-20840-z.

11. Akraam, M., Rashid, T. & Zafar, S. “An image encryption scheme proposed by modifying chaotic tent map using fuzzy numbers”. *Multimed Tools Appl*. 2023; 82: 16861–16879, https://www.scopus.com/pages/publications/85140648294?origin=resultslist.
DOI: https://doi.org/10.1007/s11042-022-13941-6.

12. 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 Information Technology.* 2026; 9 (1): 9–19, https://www.scopus.com/pages/publications/105031919219?origin=resultslist. DOI: https://doi.org/10.15276/hait.09.2026.01.

13. Järpe, E. “An alternative Diffie-Hellman protocol”. *Cryptography.* 2020; 4 (1); 5. DOI: https://doi.org/10.3390/cryptography4010005.

14. Dzurenda, P., Ricci, S., Hajny, J. & Malina, L. “Performance analysis and comparison of different elliptic curves on smart cards”. *15th Annual Conference on Privacy, Security and Trust (PST)*. Calgary, AB, Canada. 2017. p. 365–36509, https://www.scopus.com/pages/publications/85055883380?origin=resultslist. DOI: https://doi.org/10.1109/PST.2017.00050.

15. Kim, K. H., Mesnager, S. & Pak, K. I. “Montgomery curve arithmetic revisited”. *J Cryptogr Eng*. 2024; 14: 343–362, https://www.scopus.com/pages/publications/85192795289?origin=resultslist. DOI: https://doi.org/10.1007/s13389-024-00353-5.

16. Skuratovskii, R. & Osadchyy, V. “Elliptic and Edwards Curves Order Counting Method”. *International Journal of Mathematical Models and Methods in Applied Sciences*. 2021; 15: 52–62. DOI: https://dx.doi.org/10.46300/9101.2021.15.8.

17. Pope, G., Reijnders, K., Robert, D., Sferlazza, A. & Smith, B. “Simpler and faster pairings from the montgomery ladder”. *IACR Communications in Cryptology*. 2025; 2 (2). DOI: https://dx.doi.org/10.62056/ah2i893y6.

18. Burmester, M. “Group key agreement”. In J*ajodia, S., Samarati, P., Yung, M. (eds) Encyclopedia of Cryptography, Security and Privacy*. Springer, Cham. 2025. p. 1038–1045, https://www.scopus.com/pages/publications/105002554309?origin=resultslist. DOI: https://doi.org/10.1007/978-3-030-71522-9_320.

19. Muchtadi-Alamsyah, I. & Bhakti Wira Tama, Y. “Implementation of Elliptic Curve25519 in Cryptography”. In *Kehdinga George Fomunyam (ed.), Theorizing STEM Education in the 21st Century, IntechOpen*. 2020. DOI: https://doi.org/10.5772/intechopen.88614.

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 15.01.2025
Received after revision 12.03.2026
Accepted 18.03.2026

DOI: https://doi.org/10.15276/aait.09.2026.14
УДК 004.056

Метод оперативного обміну конфіденційними зображеннями для групи довірених користувачів

Хамітов Віталій Миколайович[1)]
ORCID: https://orcid.org/0009-0001-3045-8245; hamitov@op.edu.ua. Scopus Author ID: 58309128700
Болтьонков Віктор Олексійович[1)]
ORCID: https:// orcid.org/0000-0003-3366-974X; vaboltenkov@gmail.com. Scopus Author ID: 57203623617
Антощук Світлана Григорівна[1)]
ORCID: https://orcid.org/0000-0002-9346-145X; asg@opu.ua. Scopus Author ID: 8393582500
[1)] Національний університет «Одеська політехніка», пр. Шевченка, 1. Одеса, 65044, Україна

АНОТАЦІЯ

Шифрування зображень високої роздільної здатності відіграє ключову роль у забезпеченні їх конфіденційності та цілісності. Враховуючи стрімке зростання трафіку таких зображень у відкритих каналах зв'язку, розробка нових методів та засобів їхнього захисту стає все **більш актуальною**. **Метою даного дослідження** є розробка та моделювання методу обміну конфіденційними зображеннями для групи довірених користувачів. У процесі дослідження застосовувалися **методи шифрування** з хаотичними відображеннями, криптографії на еліптичних кривих, узгодження загального секрету за різними протоколами. Однією з вимог до методу, що розробляється, є його функціонування в масштабі часу, близькому до

реального. Це пов'язано зі швидким старінням інформації у зображеннях, що підлягають аналізу у групі. В основу дослідження покладено метод генерації псевдовипадкової послідовності за допомогою модифікованого хаотичного відображення Тент. Короткий ключ, який містить параметри цього відображення, передається довіреним користувачам, які утворюють групу. Далі кожен користувач може розгорнути ключ у псевдовипадкову послідовність та зашифрувати/розшифрувати зображення шифром Вернама . Група довірених користувачів формується за протоколом Діффі-Хеллмана або за протоколом Бурместера-Десмедта на еліптичних кривих. Проаналізовано з погляду обчислювальних витрат криві Вейєрштрасса, Монтгомері та Едвардса. Як робоча еліптична крива обрана крива Монтгомері як найбільш економічна в обчислювальному відношенні. Для передачі до групи довірених користувачів короткий ключ відображення Тент шифрується блоковим шифром із загальним секретом в якості ключа. Розроблений метод промодельовано для кривої Монтгомері Curve25519. Безпека зображень та їх конфіденційність забезпечується п'ятьма рівнями захисту. **В результаті встановлено**, що формування групи за протоколом Бурместера-Десмедта забезпечує роботу методу у масштабі часу, близькому до реального, та високий рівень масштабування.

Ключові слова: хаотичне перетворення Тент; шифр Вернама; протокол Діффі-Хеллмана; протокол Бурместера-Десмедта; еліптична крива Монтгомері

ABOUT THE AUTHORS

Vitaly M. Khamitov - PhD student, Department of Information Systems. Odesa Polytechnic National University, 1, Shevchenko 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

Viktor O. Boltenkov - PhD, Associate Professor, Department of Information Systems. 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

Svitlana G. Antoshchuk - Doctor of Engineering Sciences, Professor Department of Information Systems. 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 кафедри Інформаційних систем. Національний університет «Одеська Політехніка», пр. Шевченка, 1. Одеса, 65044,,Україна