УДК 004.056

М. С. Ціхоцький

МЕТОД РОЗПОДІЛУ ЗАШИФРОВАНОГО ЗОБРАЖЕННЯ ЗА (*k*,*n*)-СХЕМОЮ З ВИКОРИСТАННЯМ КОАЛІЦІЙ УЧАСНИКІВ

Вінницький національний технічний університет

Анотація

Запропоновано метод розподілу зашифрованого зображення за (k,n)-схемою з використанням коаліцій учасників. Метод передбачає поділ зашифрованого вектора на блоки, формування множини коаліцій потужності k, призначення блоків часткам учасників за комбінаторним правилом та використання дилерської частки під час відновлення. Кожен блок зашифрованого вектора пов'язується з однією коаліцією учасників і не включається до часток учасників цієї коаліції, що дозволяє зменшити обсяг індивідуальних часток порівняно з підходами, у яких кожному учаснику передається повний обсяг зашифрованих даних. Відновлення виконується допустимою коаліцією учасників: після об'єднання її часток відсутнім залишається один блок, який обчислюється з використанням дилерської частки. Така побудова забезпечує порогову умову відновлення та зменшує обсяг даних, що передаються або зберігаються окремими учасниками.

Ключові слова: розподіл секрету, (*k*,*n*)-схема, коаліція учасників, дилер, зашифрований вектор, захист зображень.

Abstract

A method for distributing an encrypted image using a (k,n)-scheme based on participant coalitions is proposed. The method involves dividing the encrypted vector into blocks, forming a set of coalitions of size k, assigning blocks to participant shares according to a combinatorial rule, and using a dealer share during recovery. Each block of the encrypted vector is associated with one participant coalition and is not included in the shares of the participants of this coalition, which reduces the size of individual shares compared with an approach in which each participant receives the full amount of encrypted data. Recovery is performed by an admissible coalition of participants: after combining their shares, one block remains missing and is computed using the dealer share. This construction provides threshold recovery and reduces the amount of data transmitted or stored by individual participants.

Keywords: secret sharing, (*k*,*n*)-scheme, participant coalition, dealer, encrypted vector, image protection.

Вступ

У системах зберігання та передавання даних повний вміст зображення не завжди має зберігатися в одному місці або передаватися одному учаснику як цілісний об'єкт. Компрометація окремого вузла або окремої частки в такому випадку не повинна призводити до відновлення всього зображення. Для цього використовують схеми розподілу секрету [1], в яких дані поділяються на частки, а відновлення виконується лише за участі визначеної множини учасників.

У пороговій схемі (*k*,*n*) секрет розподіляється між *n* учасниками так, щоб будь-яка множина з *k* учасників могла його відновити, а множина з меншою кількістю учасників не мала достатніх даних для відновлення [2]. Один із варіантів реалізації (*k*,*n*)-схеми було розглянуто в роботі [3], де частини секрету формуються за циклічним правилом, а відновлення виконується за участі дилера.

Для задач розподілу зображень важливим є не лише виконання порогової умови, а й обсяг часток, що передаються або зберігаються окремими учасниками. Якщо кожна частка має обсяг повного зашифрованого вектора, або більший то сумарний обсяг розподілених даних зростає пропорційно кількості учасників. Тому актуальною є розробка методу, у якому кожен учасник отримує тільки частину зашифрованого вектора, а будь-яка допустима коаліція з k учасників зберігає можливість відновлення

повного вектора. У цій роботі пропонується спосіб формування часток, при якому блоки зашифрованого вектора призначаються учасникам відповідно до множин коаліцій потужності *k*.

Метою роботи є розробка методу розподілу секретного вмісту зображень за (*k*,*n*)-схемою, у якій структура часток визначається множинами коаліцій учасників, а відновлення виконується з використанням дилерської частки.

Результати дослідження

Нехай задано множину учасників:

$$\mathbf{U} = \{U_1, U_2, ..., U_n\},$$

де *n* – загальна кількість учасників. Для методу приймається умова $2 \le k < n$, де *k* – мінімальна кількість учасників, необхідна для відновлення зашифрованого зображення.

Оскільки, даний підхід, на відміну від інших, відрізняється відносною просторою операцій під час розподілу, розподіл відкритого зображення не захищав би його конфіденційність. Тому пропонується попередньо шифрувати зображення за методом [4]. Отже, після зашифрування отримуємо зашифрований вектор **C**, який необхідно поділити на *m* блоків:

$$\mathbf{C} = \{C_1, C_2, ..., C_m\}.$$

Кількість таких блоків визначається кількістю всіх можливих коаліцій із *k* учасників:

$$m = \binom{n}{k} = \frac{n!}{k!(n-k)!}.$$

Такий вибір кількості блоків пов'язує кожен блок зашифрованого вектора з однією коаліцією учасників потужності *k*. У роботах [5, 6] автори вказують на можливість такої організації порогових схем розподілу.

Для визначення правила розміщення блоків формується множина індексів учасників та на її основі будується впорядкований набір індексних множин:

$$\mathbf{G} = \{G_1, G_2, ..., G_m\}.$$

Кожна множина G_j містить *k* різних індексів і відповідає одній коаліції учасників. Кожному блоку C_j ставиться у відповідність одна множина G_j. Ця множина визначає, у частках яких учасників блок C_j буде відсутній. Побудова набору G задає структуру доступу через усі коаліції потужності *k*, що узгоджується з підходами до побудови схем для складніших структур доступу [7].

Частка учасника U_q формується за правилом:

$$P_q = \{C_j \mid q \notin G_j\}.$$

Тобто блок C_j не включається до часток тих учасників, індекси яких входять до множини G_j, і включається до часток усіх інших учасників. У результаті кожен блок відсутній рівно у *k* частках і наявний у частках решти *n*−*k* учасників. Для зображень така побудова є важливою, оскільки дозволяє формувати частки меншого обсягу порівняно з підходами, у яких кожен учасник отримує повний обсяг зашифрованих даних [8].

Додатково формується дилерська частка *D*, яка не входить до складу жодної частки учасника. Вона обчислюється як сума за модулем 2 усіх блоків зашифрованого вектора:

$$D = C_1 \oplus C_2 \oplus ... \oplus C_m.$$

Саме з рахунок поєднання такої побудови схеми розподілу та використання дилера дозволяє забезпечити зменшення обсягу часток які надаються окремим учасникам схеми.

Для відновлення зображення розглядається отримана коаліція часток/учасників, перевіряється які саме блоки наявні серед усіх часток і якого не вистачає. Після об'єднання часток учасників коаліції формується набір усіх блоків зашифрованого вектора, крім одного блока C_s. Відсутній блок обчислюється з використанням дилерської частки:

$$C_s = D \oplus \bigoplus_{\substack{j=1,\\ j\neq s}}^{m} C_j .$$

Після обчислення блока C_s формується повний набір блоків $\mathbf{C} = \{C_1, C_2, ..., C_m\}$.

Якщо доступними є менш ніж *k* часток, то після їх об'єднання відсутніми залишаються два або більше блоків. Оскільки дилерська частка *D* задає лише одну залежність між усіма блоками, вона не дозволяє однозначно визначити кілька невідомих складових. У такому випадку повне відновлення зашифрованого вектора не виконується.

Розглянемо приклад застосування такого методу розподілу для схеми $k = 2,\ n = 4$.

Згідно з правилом розбиття, кількість блоків *m* дорівнює 6: $\mathbf{C} = C_1, C_2, C_3, C_4, C_5, C_6$. Далі необхідно сформувати правило вибору блоків C_j (*j*=1, 2, …6) до часток P_i (*i*=1, 2, 3, 4) на основі визначення допустимих множин індексів:

$$G_1 = \{1,2\},\ G_2 = \{1,3\},\ G_3 = \{1,4\},\ G_4 = \{2,3\},\ G_5 = \{2,4\},\ G_6 = \{3,4\}.$$

Як бачимо з прикладу, множини індексів **G** забезпечують повне покриття усіх блоків *C* таким чином, що кожен набір індексів зустрічається тільки один раз. На основі значень цих множин виконується формування часток учасників *P*:

$$P_1 = \{C_4, C_5, C_6\},\ P_2 = \{C_2, C_3, C_6\},\ P_3 = \{C_1, C_3, C_5\},\ P_4 = \{C_1, C_2, C_4\}.$$

Частки *P* були сформовані таким чином, що в кожну частку входять тільки ті блоки *C* індекс яких відсутній у множині G_j.

Аналізуючи перетин будь-яких *k* часток **P** бачимо, що вони спроможні сформувати таку послідовність блоків C_j, при якому завжди буде не вистачати одного блоку. Коаліція $A = \{U_1, U_3\}$ акумулює частки $P_1 = \{C_4, C_5, C_6\}$ та $P_3 = \{C_1, C_3, C_5\}$, при яких формується $C = C_1, C_3, C_4, C_5, C_6$. В такому випадку відсутнім блоком є C_2, значення якого ми можемо відновити з використання частки дилера *D*:

$$C_2 = D \oplus C_1 \oplus C_3 \oplus C_4 \oplus C_5 \oplus C_6 .$$

На даному етапі визначена коаліція учасників за участю дилера вже може відновити зашифрований вектор **C**. При цьому, якщо розглянути випадок коли коаліція налічує *k*–1 учасників, то відновлення відсутнього блоку з використанням частки дилера є неможливим, оскільки вона не може відновити 2 чи більше невідомих складових.

Висновки

Запропонований метод розподілу зашифрованого зображення використовує відповідність між блоками вектора *C* і коаліціями учасників потужності *k*. За цим правилом кожен блок не включається до часток однієї коаліції та включається до часток решти учасників. Завдяки цьому будь-яка допустима коаліція з *k* учасників після об'єднання своїх часток має всі блоки, крім одного, а відсутній блок відновлюється за допомогою дилерської частки *D*. Додатково було встановлено що запропонована схема розподілу забезпечує зменшення обсягу розподілених даних. Якщо доступними є менш ніж *k* часток, після їх об'єднання відсутніми залишаються два або більше блоків, тому однієї дилерської частки недостатньо для повного відновлення. Отже, метод забезпечує порогову умову відновлення, зменшує обсяг індивідуальних часток і задає процедуру відновлення зашифрованого вектора через визначення коаліції.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Ціхоцький М. С., Лужецький В. А. Аналіз методів розподілу секрету // Кібербезпека: освіта, наука, техніка. 2024. Т. 1, № 25. С. 279–293. URL: https://doi.org/10.28925/2663-4023.2024.25.279293 (дата звернення: 10.01.2026).
2. Shamir A. How to Share a Secret // Communications of the ACM. 1979. Vol. 22, No. 11. P. 612–613. URL: https://doi.org/10.1145/359168.359176 (дата звернення: 12.01.2026).
3. Лужецький В. А., Ціхоцький М. С. Схема порогового розподілення секрету (k, n) // ІТКМ IEEE. Івано-Франківськ, 2024. Сек. 5(24). С. 147–148. ISBN 978-966-640-560-2. URL: https://journal.compsc.if.ua/test/public/journals/zbirnyk_2024.pdf (дата звернення: 12.01.2026).
4. Luzhetskyi V., Tsikhotskyi M. Image encryption and distribution method based on LFSR and counters // Information Technologies and Computer Engineering. 2025. Vol. 22, No. 3. P. 77–88. URL: https://doi.org/10.31649/vitce/3.2025.77 (дата звернення: 14.01.2026).
5. Ito M., Saito A., Nishizeki T. Multiple assignment scheme for sharing secret // Journal of Cryptology. 1993. Vol. 6. P. 15–20. URL: https://doi.org/10.1007/BF02620229 (дата звернення: 15.01.2026).
6. Masucci B. Sharing Multiple Secrets: Models, Schemes and Analysis // Designs, Codes and Cryptography. 2006. Vol. 39. P. 89–111. URL: https://doi.org/10.1007/s10623-005-2761-1 (дата звернення: 19.01.2026).
7. Chen Q., Ren X., Hu L., Cao Y. Ideal uniform multipartite secret sharing schemes // Information Sciences. 2024. Vol. 655. Article 119907. URL: https://doi.org/10.1016/j.ins.2023.119907 (дата звернення: 20.01.2026).
8. Saha S., Chattopadhyay A. K., Barman A. K., Nag A., Nandi S. Secret Image Sharing Schemes: A Comprehensive Survey // IEEE Access. 2023. Vol. 11. P. 98333–98361. URL: https://doi.org/10.1109/ACCESS.2023.3304055 (дата звернення: 22.01.2026).

Ціхоцький Микита Сергійович – аспірант групи 125-22а, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, Україна ORCID ID: 0009-0005-8101-3536 e-mail: nik.tsikhotskiy15@gmail.com

Tsikhotskyi Mykyta – Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: nik.tsikhotskiy15@gmail.com