РАДІОТЕХНІКА ТА ТЕЛЕКОМУНІКАЦІЇ

УДК 004.622: 517.927
DOI https://doi.org/10.32782/2663-5941/2026.1.1/06

Бараннік В.В.
https://orcid.org/0000-0002-2848-4524
Харківський національний університет радіоелектроніки

Прокопенко Р.О.
https://orcid.org/0009-0006-0789-9073
Харківський національний університет радіоелектроніки

МЕТОД СТЕГАНОГРАФІЧНИХ ПЕРЕТВОРЕНЬ В ПОЗИЦІЙНОМУ ПРОСТОРІ

В статті обґрунтовується те, що в умовах активної протидії з боку протиборчої сторони виникають складнощі в процесі забезпечення безпеки відеоінформації, яка передається з використанням інформаційно-комунікаційних систем з борового комплексу. В основі наукової проблематики тут кроїться суперечність між вимогами до зменшення бітового об'єму та забезпеченням конфіденційності та цілісності інформації. В статті показано, що одним з підходів для захисту відеоінформації є методи стеганографії. Відмінна перевага тут стосується можливості захисту інформації шляхом приховування у відео-контейнерах без руйнації його змісту. Базовим методом, який має найбільш поширене практичне застосування та апробацію є метод вбудовування до найменш значимого біту двійкового синтаксису контейнеру. Метод LSB відноситься до класу методів безпосередньої заміни. В статті показується, що одним з перспективних є розвиток методів вбудовування інформації з використанням механізму LSB у квантованому спектральному просторі. В цьому разі інформація приховується в найменш значимі бітові групи коефіцієнтів дискретного косинусного перетворення. Даний варіант приховування інформації методом LSB має більше практичне застосування. Однак для нього притаманний дисбаланс між: об'ємом інформації, що вбудовується (стеганографічна ємність); значенням коефіцієнта стиснення сегментів-ВКН. Такий дисбаланс зумовлено тим, що за рахунок вбудовування інформації змінюються або частково руйнуються вагомі особливості, які використовуються в процесі подальшого стиснення. Надається обґрунтування того, що для подальшого розвитку методів стеганографії пропонується використовувати підходи, які базуються на встановлені функціональних залежностей в області виявлення структурних ознак. Розробляється метод стеганографічних перетворень в структурному просторі на основі модифікації П-базису за умов виявлення відповідних ознак в спектрально-квантованому описі відеосегментів. Доводиться перевага створеного методу за кількістю вбудованої інформації в умовах заданого рівня маскування факту наявності прихованої інформації.

Ключові слова: *роботизовані комплексні, контейнери візуального походження, скорочення надмірності, структурні залежності, позиційний базис.*

Постановка проблеми. Забезпечення безпеки інформаційних ресурсів складає важливу проблематику. Особливо це стосується умов активної протидії з боку протиборчої сторони [1, с. 4]. Водночас в процесі вирішення таких питань виникають складнощі. Характерним прикладом тут є доставка відеоінформації з бортових комплексів. В цьому випадку існує множина вразливих факторів. До них слід віднести наступні [2, с. 22]:

– обмеженість енергетичних ресурсів бортових комплексів;

– недостатня щодо сучасних вимог швидкість передачі даних з бортових комплексів;

– існування ризиків перехвату інформаційного потоку або управління бортовим комплексом [3, с. 15].

За означеними обставинами з одного боку підвищується вимоги щодо захисту інформації. З іншого боку підвищуються вимоги відносно зменшення бітового об'єму відеоінформаційного потоку. Одночасне забезпечення таких вимог в умовах оброки та передачі інформації з застосуванням бортових комплексів є нетривіальною науково-прикладною задачею [4, с. 4]. Отже забезпечення рівня захисту інформації в умовах її своєчасної передачі з використанням бортових комплексів є актуальною ***науково-прикладною задачею***.

Аналіз останніх досліджень і публікацій. Для захисту інформації щодо несанкціонованого доступу використовують два підходи [5, с. 10].

Перший – використовуються метоли криптографічного шифрування. Такий варіант пов'язано зі збільшенням об'єму бітового опису відеоданих. Причиною чого є додаткова формування бітового об'єму для передачі перевірочних (контрольних) послідовностей в процесі реалізації завадостійкого кодування [6, с. 3].

Другий підхід стосується використання методів стеганографії. Відмінна перевага тут стосується можливості захисту інформації шляхом приховування у відео-контейнерах [7, с. 2] без руйнації його змісту. Відповідно виникає потреба щодо практичного застосування даного підходу в комплексних системах для підвищення рівня конфіденційності інформації.

Базовим методом, який має найбільш поширене практичне застосування та апробацію є метод вбудовування до найменш значимого біту двійкового синтаксису контейнеру [8, с. 3]. Англомовне позначення такого методу – LSB. Метод LSB відноситься до класу методів безпосередньої заміни.

Одним з перспективних є розвиток методів вбудовування інформації з використанням механізму LSB у квантованому спектральному просторі. В цьому разі інформація приховується в найменш значимі бітові групи коефіцієнтів дискретного косинусного перетворення [9, с. 5].

Даний варіант приховування інформації методом LSB має більше практичне застосування. Однак для нього притаманний дисбаланс між: об'ємом інформації, що вбудовується (стеганографічна ємність); значенням коефіцієнта стиснення сегментів-ВКН [10, с. 4].

Такий дисбаланс зумовлено тим, що за рахунок вбудовування інформації змінюються або частково руйнуються вагомі особливості, які використовуються в процесі подальшого стиснення. Наприклад, можуть руйнуватися: серії з елементів матриці ДКП, які мають нульові значення; статистичні залежності в напрямку вирівнювання законів розподілу. Звідси втрачається ефективність процесів усунення статистичної та структурної надмірності. Стандартизовано для існуючих підходів обмеження такого дисбалансу досягається шляхом скорочення об'єму інформації, яка приховується.

Основним недоліком тут є залежність кількості вбудованої інформації від рівня маскування факту такого приховування [11, с. 3].

Постановка завдання. Для подальшого розвитку методів стеганографії пропонується використовувати підходи, які базуються на встановлені функціональних залежностей в області виявлення структурних ознак [12, с. 5]. Варіантом тут може бути використання в якості базового підходу методу модифікацій у позиційному базисі (П-базисі). Отже ***мета статті*** стосується розробки методу стеганографічних перетворень в структурному просторі трансформованих сегментів-контейнерів.

Виклад основного матеріалу. Стеганографічна система шляхом перетворень в НРВ базисі включає наступні складові (пряме та зворотне перетворення):

І. ***Пряме перетворення***. Стеганографічне вбудовування інформації на основі функціональних перетворень з модифікацією адаптивного позиційного базису. Такі перетворення застосовуються до окремих адаптивних позиційних чисел або до всього ВП-контейнеру. Блок-схема етапів стеганографічного вбудовування представлена на рис 1.

Вбудовування інформаційного біту λ_ξ згідно особливостей функціональних перетворень в П-базисі. Тут виконуються такі дії:

– здійснення модифікації ОПЧ $r_{i,j}$ в межах допустимої зміни за умов зменшення впливу на рівень стиснення (зменшення кількості H_j штучної надмірності, тобто $\eta=1$);

– вбудовування біту λ_ξ повідомлення Λ шляхом використання механізму модифікації ОПЧ $r_{i,j}$ за умов виключення втрат цілісності та зменшення впливу на рівень стиснення. Для цього застосовується правило:

$$r'_{i,j} = \min\left(\max\{S(\alpha;\beta)_j\};\delta_i\right)+\theta|\ \theta = 1+sign(\lambda_\xi).$$

Після чого організується знаходження значення коду N'_j за обліком модифікованого значення ОПЧ $r'_{i,j}$ в П-базисі. Тут відбувається стис-

Рис. 1. Схема послідовності етапів стеганографічного вбудовування в адаптивному П-базисі

нення ВП-контейнеру з використанням сукупності залежностей його змісту одночасно для скорочення надмірності та приховування інформації. Для цього з врахуванням модифікованої величини ОПЧ $r'_{i,j}$ застосовується формула:

$$N'_j = \sum_{i=1}^{m} s_{i,j} \cdot f_{wc}(\Omega_j; r'_{i,j}|\sigma=0) = \sum_{i=1}^{m} s_{i,j} \cdot W'(\sigma=0)_{i,j}$$

де $s_{i,j}$ – елемент АПЧ в П-базисі;

$f_{wc}(\Omega_j; r'_{i,j}|\sigma=0)$ – функціонал визначення вагових коефіцієнтів з врахуванням модифікації ОПЧ в П-базисі за умов $(r'_{i,j}|\sigma=0)$ нівелювання впливу на втрату інформації за показником середньоквадратичного відхилення σ;

$W'(\sigma=0)_{i,j}$ – ваговий коефіцієнт для i-го елементу ВП-контейнеру за умов виключення впливу стеганографічних перетворень на цілісність елементів ВП-контейнеру.

Зворотне перетворення. Розглянемо процес вилучення вбудованих даних. В загалі для комплексної системи такий процес реалізується двома етапами.

Перший етап – вилучення прихованої інформації під час відновлення ВП-контейнеру на основі декомпресії в П-базисі. Такий процес здійснюється в загальному випадку в двох концепціях:

1) у разі стеганографічних перетворень без залучення стеганографічного ключа (наприклад, використовується лише ключ для криптографічного шифрування інформації перед вбудовуванням);

2) у разі використання стеганографічного ключа.

Кожна з таких концепцій розглядається за умов застосування режимів авторизованого та неавторизованого доступу. Найбільший рівень захисту досягається у разі додаткового застосування стеганографічного ключа.

За умов авторизованого режиму доступу на приймальній стороні вважається відомим стеганографічний ключ. Звідси процес декодування та вилучення має доступ до відомостей щодо: правила вбудовування та порядку розподілу прихованої інформації за ВП-контейнерами; значення початкових елементів хаотичних послідовностей. Функціональна-схема етапів процесу вилучення прихованої інформації в П-базисі під час декомпресії ВП-контейнера представлена на рис. 2.

Приріст за кількістю вбудованих даних для розробленого методу відносно існуючих підходів надано в табл. 1. Розрахунки проводяться в режимах: без обліку результатів процесу стиснення вбудованих даних та ВП-контейнеру; врахування попереднього стиснення ВП-контейнеру.

З огляду на дані, що надано в табл. 1, можна заключити те, що досягається перевага для розробленого методу стегано-перетворень за кількістю вбудованої інформації до ВП-контейнеру. Такі результати отримано в процесі проведення експериментальних досліджень в умовах забезпечення заданого рівня маскування факту наявності стегано-перетворень. При цьому означена

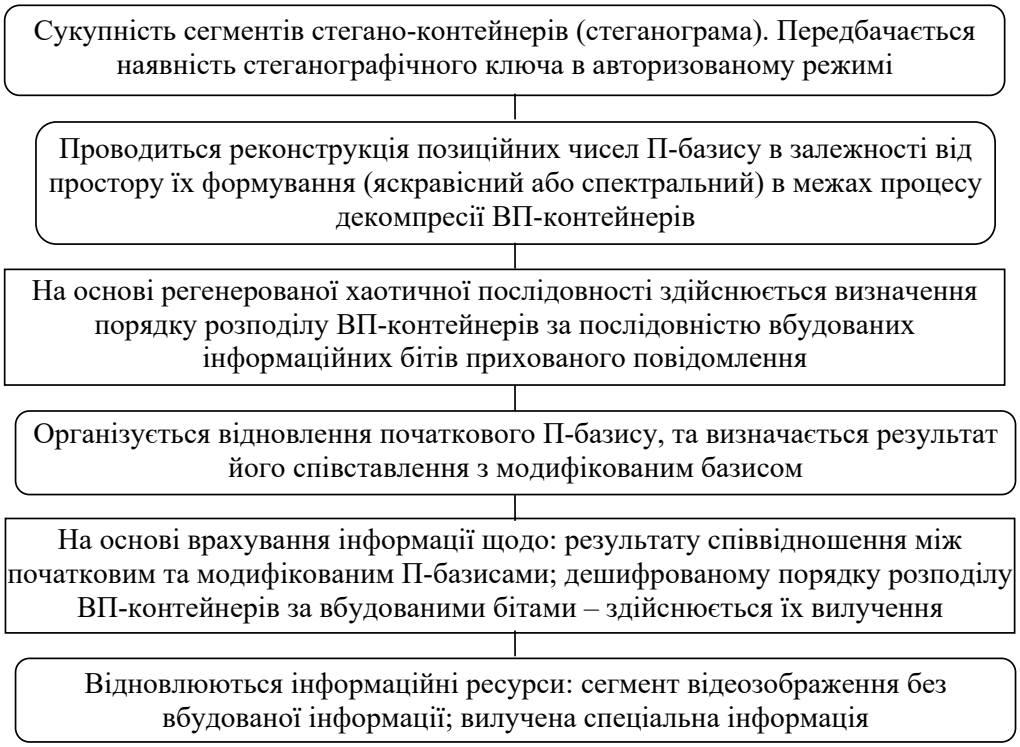

Рис. 2. Функціональна схема вилучення прихованої інформації під час декомпресії ВП-контейнеру в П-базисі з використанням компонент стеганографічного ключа щодо їх розподілу

Таблиця 2

Приріст за величиною стеганографічної ємності v_{hid} для створеної комплексної системи відносно існуючих підходів, %

Розмір $m \times n$ відео-контейнеру	**v_{hid}, біт/ піксель, %**	**v_{hid} біт/піксель, % (у разі стиснення відеоданих-контейнерів)**
4×4	7	14
6×6	4	8
8×8	2	5

перевага в залежності від розміру ВП-контейнеру має такі оцінки: в режимі без врахування процесів стиснення ВП-контейнерів в середньому 5 % ; в режимі стиснення ВП-контейнерів та прихованої інформації в середньому на 10 %.

Висновки. 1. Розроблено метод стеганографічних перетворень в структурному просторі на основі модифікації П-базису за умов виявлення відповідних ознак в спектрально-квантованому описі відеосегментів.

2. Доведена перевага створеного методу за кількістю вбудованої інформації в умовах заданого рівня маскування факту наявності прихованої інформації.

Список літератури:

1. Sharma R., Bollavarapu S. Data Security using Compression and Cryptography Techniques. *International Journal of Computer Applications*. 2015. Vol. 117. No. 14. P. 15–18. DOI: https://doi.org/10.5120/20621-3342

2. Dipankar D. Comparative Analysis of Steganographic Techniques for Data Hiding in Digital Images. *Journal contribution*. 2025. DOI: https://doi.org/10.6084/m9.figshare.30621860.v1

3. Ravindra A., Bansod S., Singh S. K. LSB-Based Image Steganography Using Image Enlargement. *Computing Technologies (ICOCT)*: Proceedings International Conference, Bengaluru, India, 2025, P. 1–4. DOI: https://doi.org/10.1109/ICOCT64433.2025.11118799

4. Barannik D., Barannik V. Steganographic Coding Technology for Hiding Information in Infocommunication Systems of Critical Infrastructure. *Advanced Trends in Information Theory (ATIT)*: Proceedings IEEE 4th International Conference Kyiv, Ukraine. 2022. P. 88–91. DOI: https://doi.org/10.1109/ATIT58178.2022.10024185.

5. Bas P., Filler T., and Pevný T. Break our steganographic system – the ins and outs of organizing BOSS. In T. Filler, T. Pevný, A. Ker, and S. Craver, editors, Information Hiding, 13th International Conference. – vol.6958 of Lecture Notes in Computer Science. pp. 59-70. Prague, Czech Republic. 2011. DOI: https://doi.org/10.1007/978-3-642-24178-9_5

6. A Method of Scrambling for the System of Cryptocompression of Codograms Service Components / Barannik, V. et al. In: Klymash, M., et al. Emerging Networking in the Digital Transformation Age. Lecture Notes in Electrical Engineering, vol 965. Springer, Switzerland, Cham, 2022. DOI: https://doi.org/10.1007/978-3-031-24963-1_26.

7. Основи теорії структурно-комбінаторного стеганографічного кодування: монографія / В.В. Бараннік та ін. Харків: Видавництво «Лідер», 2017. 256 с.

8. Barannik V., Alimpiev A., Barannik D., Barannik N. Detections of sustainable areas for steganographic embedding. *East-West Design & Test Symposium (EWDTS)*: Proceedings IEEE 4th International Conference. 2017, P. 555–558. DOI: https://doi.org/10.1109/EWDTS.2017.8110028.

9. Бараннік Д.В. Метод двокаскадної імплантації прихованої інформації на основі стеганокомпресійних перетворень. *Інформаційні технології та електронна інженерія*. 2024. № 1. С. 31–38.

10. Barannik V., Shiryaev A. Quadrature compression of images in polyadic space. *Modern Problem of Radio Engineering, Telecommunications and Computer* Science: Proceedings of International Conference. 2012, P. 422–422. INSPEC Accession Number: 12713484.

11. Бараннік Д.В. Технологія приховування інформативного контенту в динамічному потоці відеосегментів. *Наукоємні технології*. 2023. № 4. С. 408–415. DOI: https://doi.org/10.18372/2310-5461.60.18270.

12. Barannik V., Khimenko V., Barannik N. Method of indirect information hiding in the process of video compression. *Radioelectronic and Computer Systems*. 2021. №. 4. P. 119–131. DOI: https://doi.org/10.32620/reks.2021.4

Barannik V.V., Prokopenko R.O. THE METHOD OF STEGANOGRAPHIC TRANSFORMATIONS IN POSITIONAL SPACE

The article substantiates the fact that in conditions of active counteraction from the opposing side, difficulties arise in the process of ensuring the security of video information transmitted using information and communication systems from the boron complex. The basis of the scientific problem here is the contradiction between the requirements for reducing the bit volume and ensuring the confidentiality and integrity of information. The article shows that one of the approaches to protecting video information is steganography methods. A distinct advantage here concerns the possibility of protecting information by hiding it in video containers without destroying its content. The basic method, which has the most widespread practical application and testing, is the method of embedding in the least significant bit of the binary syntax of the container. The LSB method belongs to the class of direct substitution methods. The article shows that one of the promising ones is the development of methods for embedding information using the LSB mechanism in quantized spectral space. In this case, information is hidden in the least significant bit groups of the coefficients of the discrete cosine transform. This variant of information hiding using the LSB method has more practical application. However, it is characterized by an imbalance between: the amount of information being embedded (steganographic capacity); the value of the segment compression coefficient-VKN. Such an imbalance is due to the fact that due to the embedding of information, important features that are used in the process of further compression are changed or partially destroyed. The justification is provided for the fact that for the further development of steganography methods it is proposed to use approaches based on the establishment of functional dependencies in the field of detecting structural features. A method of steganographic transformations in structural space is developed based on the modification of the P-basis under the conditions of detecting the corresponding features in the spectral-quantized description of video segments. The advantage of the created method in terms of the amount of embedded information under the conditions of a given level of masking of the fact of the presence of hidden information is proved.

Keywords: *robotic complex, containers of visual origin, redundancy reduction, structural dependencies, positional basis.*

Дата першого надходження статті до видання: 09.01.2026
Дата прийняття статті до друку після рецензування: 04.02.2026
Дата публікації (оприлюднення) статті: 08.04.2026