

# ПІДВИЩЕННЯ ЗАХИЩЕНОСТІ ДАНИХ ТОЧНОГО ЗЕМЛЕРОБСТВА ГІБРИДНОЮ СТЕГАНОГРАФІЄЮ НА ОСНОВІ МЕТОДІВ HMPSO ТА DDV

Вінницький Національний Технічний Університет

## **Анотація**

*Запропоновано гібридний метод стеганографічного захисту даних у системах точного землеробства. Метод поєднує алгоритм HMPSO для оптимального вибору пікселів зображення-контейнера та алгоритм DDV для безпосереднього вбудовування секретних даних. Перед вбудовуванням секретне повідомлення стискається за допомогою кодування Хаффмана. Запропонований підхід забезпечує високий рівень конфіденційності та цілісності даних, зібраних з бездротових сенсорних мереж, при збереженні енергоефективності та візуальної якості стеганоконтейнера. Проведено порівняльний аналіз з існуючими рішеннями у сфері захищеної агрегації даних точного землеробства.*

**Ключові слова:** стеганографія, точне землеробство, HMPSO, DDV, бездротові сенсорні мережі, конфіденційність даних.

## **Abstract**

*A hybrid steganography method for data protection in precision agriculture systems is proposed. The method combines the HMPSO algorithm for optimal selection of image container pixels and the DDV algorithm for direct embedding of secret data. Before embedding, the secret message is compressed using Huffman coding. The proposed approach ensures a high level of confidentiality and integrity of data collected from wireless sensor networks while maintaining energy efficiency and visual quality of the stegancontainer. A comparative analysis with existing solutions in the field of secure data aggregation in precision agriculture is carried out.*

**Keywords:** steganography, precision agriculture, HMPSO, DDV, wireless sensor networks, data confidentiality.

## **Вступ**

У сучасних системах точного землеробства значні обсяги чутливих даних, зібраних з бездротових сенсорних мереж (температура ґрунту, вологість, вміст поживних речовин, дані з дронів тощо), передаються для подальшої агрегації та аналізу. Захист цих даних від несанкціонованого доступу є критичним завданням, оскільки витік інформації може призвести до економічних збитків та порушення конфіденційності [1].

Традиційні криптографічні методи захисту даних створюють додаткове навантаження на обмежені енергетичні ресурси сенсорних вузлів, що негативно впливає на загальну енергоефективність мережі. Перспективним напрямком вирішення цієї проблеми є застосування стеганографії, яка дозволяє приховувати секретні дані всередині зображень-контейнерів без помітних візуальних змін, зберігаючи при цьому енергоресурси сенсорних пристроїв.

Існуючі підходи до захищеної агрегації даних у точному землеробстві здебільшого зосереджені на криптографічних протоколах та енергоефективній маршрутизації [1], проте недостатньо уваги приділяється гібридним стеганографічним методам, які поєднують високу імперцептивність, стійкість до стеганоаналізу та збільшену ємність вбудовування.

У роботі запропоновано гібридний стеганографічний метод захисту даних у системах точного землеробства на основі алгоритмів HMPSO та DDV, який забезпечує підвищення конфіденційності та цілісності інформації при збереженні енергоефективності бездротових сенсорних мереж.

## Дослідження

У роботі запропоновано гібридний стеганографічний метод захисту даних у системах точного землеробства, який базується на поєднанні алгоритмів HMPSO та DDV з попереднім стисненням секретного повідомлення за допомогою кодування Хаффмана [2]. Запропонований підхід спрямований на підвищення конфіденційності та цілісності чутливих даних, що передаються через бездротові сенсорні мережі, без суттєвого збільшення енергоспоживання сенсорних вузлів.

Метод включає чотири основні етапи. На першому етапі попередньої обробки секретне повідомлення, яке містить показники сенсорів (температура, вологість ґрунту, вміст поживних речовин, дані з дронів тощо), команди управління або координати, стискається за допомогою алгоритму Хаффмана. Це дозволяє суттєво збільшити ємність вбудовування секретних даних без втрати інформації та зменшити обсяг даних, що підлягають приховуванню.

На етапі вибору пікселів для вбудовування використовується алгоритм HMPSO (Hénon Map + Particle Swarm Optimization). Поєднання хаотичної динаміки карти Хенона з оптимізацією роєм частинок дає змогу ефективно уникнути передчасної збіжності до локальних оптимумів, характерної для класичного PSO. Завдяки цьому забезпечується рівномірний розподіл вбудовування по всьому зображенню-контейнеру, що підвищує стійкість до статистичних методів стеганоаналізу.

Безпосереднє вбудовування секретних бітів здійснюється за допомогою алгоритму DDV (Distinction Disparity Value). Цей метод враховує різницю інтенсивності між сусідніми пікселями, що дозволяє адаптивно визначати кількість бітів, які можна приховати в кожному пікселі без помітного погіршення візуальної якості зображення. Такий підхід забезпечує високу імперцептивність стеганозображення та покращує стійкість до пасивних атак.

Запропонований гібридний метод добре інтегрується з існуючими рішеннями захищеної агрегації даних у бездротових сенсорних мережах точного землеробства [1]. У якості контейнерів використовуються зображення, отримані від безпілотних літальних апаратів (дронів) або стаціонарних наземних камер спостереження. Це дозволяє приховувати агреговані дані сенсорів безпосередньо в зображеннях, що передаються до центру обробки, без необхідності додаткового енергоспоживання на шифрування даних на рівні окремих сенсорних вузлів.

Результати теоретичного моделювання та порівняльного аналізу свідчать, що запропонований гібридний метод HMPSO+DDV забезпечує кращі показники імперцептивності, ємності вбудовування та стійкості до виявлення прихованих даних у порівнянні з традиційними стеганографічними підходами. При цьому зберігається сумісність з вимогами енергоефективності, що є критичним для ресурсозалежних сенсорних мереж у точному землеробстві [3].

## Висновок

У роботі запропоновано гібридний стеганографічний метод захисту даних у системах точного землеробства на основі алгоритмів HMPSO та DDV з попереднім стисненням секретних повідомлень за допомогою кодування Хаффмана.

Запропонований підхід забезпечує високий рівень конфіденційності та цілісності чутливих даних, зібраних бездротовими сенсорними мережами, при збереженні візуальної якості зображень-контейнерів та енергоефективності системи в цілому. Поєднання оптимального вибору пікселів за допомогою HMPSO та адаптивного вбудовування даних за алгоритмом DDV дозволяє суттєво підвищити стійкість до пасивних стеганоаналітичних атак порівняно з традиційними методами стеганографії.

Результати дослідження підтверджують ефективність інтеграції запропонованого гібридного методу з існуючими рішеннями захищеної агрегації даних у точному землеробстві. Отримані результати відкривають перспективи для подальшого вдосконалення стеганографічних механізмів захисту інформації в ресурсозалежних IoT- та WSN-системах.

## СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Nagaraja G. S., Vanishree K., Azam F. Novel Framework for Secure Data Aggregation in Precision Agriculture with Extensive Energy Efficiency // Journal of Computer Networks and Communications. 2023. Article ID 5926294. 11 p.

2. Ali A. S., Alsamarae S., Hussein A. A. Optimize Image Steganography Based on Distinction Disparity Value and HMPSO to Ensure Confidentiality and Integrity // Journal of Computer Networks and Communications. 2024. Article ID 2516567. 15 p.

3. Карпинець В. В., Присяжний Д. П., Безпалый К. В., Білоус В. М., Тельнік Д. В. Удосконалений підхід до формування стеганоконтейнерів із застосуванням штучного інтелекту // Наукові праці Вінницького національного технічного університету. 2026. № 1.

***Калантай Анна Сергіївна*** – студентка групи 1KITC-226, факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, м. Вінниця, e-mail: anna5sunny@gmail.com

***Карпинець Василь Васильович*** – канд. техн. наук, доцент, завідувач кафедри менеджменту та безпеки інформаційних систем, Вінницький національний технічний університет, м. Вінниця, e-mail: karpinets@gmail.com

***Kalantai Anna S.*** – Student of 1KITS-22B group, Faculty of Management and Information Security, Vinnytsia National Technical University, Vinnytsia, email: anna5sunny@gmail.com

***Karpinets Vasyl V.*** – Cand. Sc. (Eng.), Associated Professor, Head of the Chair of Management and Security of Information Systems, Vinnytsia National Technical University, Vinnytsia, e-mail: karpinets@gmail.com