УДК 621.327:681.5 DOI: 10.30748/soivt.2019.60.07

І.М. Тупиця, В.В. Димчук, К.В. Чуянов, М.М. Кодацький

*Харківський національний університет Повітряних Сил ім. І. Кожедуба, Харків*

# МЕТОД ПІДВИЩЕННЯ ПРОПУСКНОЇ СПРОМОЖНОСТІ СКРИТОГО КАНАЛУ В ІНФОКОМУНІКАЦІЙНИХ СИСТЕМАХ СПЕЦІАЛЬНОГО ПРИЗНАЧЕННЯ

*Встановлено, що методи цифрової стеганографії мають ряд недоліків: низька стійкість до атак, невеликий обсяг стеганографічної ємності та є нестійкими, при передачі зображень та активних атак противника можлива втрата даних. Розвиток систем, що використовують зображення та відео для передачі даних, змушує впроваджувати методи цифрової стеганографії для захисту даних.*

***Ключові слова:*** *цифрова стеганографія, пропускна спроможність, атака, дискретне вейвлет-перетворення.*

## Вступ

Надійний захист інформації від несанкціонованого доступу є актуальною, але не вирішеною в повному обсязі проблемою. В сучасному світі широко застосовуються і бурхливо розвиваються телекомунікаційні системи в усіх сферах діяльності людини [1–7]. Тому, гостро постає питання захисту інформації. Одним з можливих рішень задачі підвищення інформаційних систем є застосування методів цифрової стеганографії [8–12].

Методи стеганографії дозволяють не тільки приховано передавати дані, але й успішно вирішувати завдання завадостійкої автентифікації, захисту інформації від несанкціонованого копіювання, відстеження поширення інформації мережами зв'язку, пошуку інформації в мультимедійних базах даних.

**Аналіз останніх досліджень і публікацій.** Проаналізувавши останні наукові публікації можна зробити висновок, що методи цифрової стеганографії мають ряд недоліків [13–16]: низька стійкість до атак, невеликий обсяг стеганографічної ємності та є нестійкими, при передачі зображень та активних атак противника можлива втрата даних.

При побудові стеганосистеми повинні враховуватись наступні положення:

– стеганосистема повинна мати прийнятну обчислювальну складність реалізації;

– методи приховування повинні забезпечувати автентичність і цілісність секретної інформації для авторизованої особи;

– потенційний порушник має повне уявлення про стеганосистему і деталі її реалізації. Єдине, що йому невідоме, – ключ, за допомогою якого тільки його власник може встановити факт наявності та зміст прихованого повідомлення;

– порушник повинен бути позбавлений будь-яких технічних та інших переваг в розпізнанні або ж принаймні розкритті змісту секретних повідомлень.

**Мета статті** – розробка методу підвищення пропускної спроможності скритого каналу для інформаційних технологій обробки та передачі відеоінформаційних ресурсів.

## Виклад основного матеріалу

Для забезпечення додаткової завадостійкості необхідно забезпечити підвищення пропускної спроможності, оскільки використання методів завадостійкого кодування чи дублювання інформації вимагає передачі додаткових біт. В ході досліджень було визначено два методи підвищення пропускної здатності при використанні методів вбудовування в область перетворення.

Перший метод базується на твердженні, що вбудовування у середньочастотні коефіцієнти ДКП забезпечить достатню стійкість зображення, оскільки вони зазвичай не піддаються модифікаціям та втратам збоку алгоритмів стиснення.

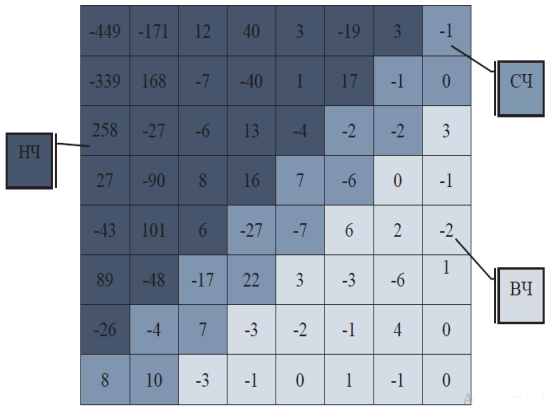


Рис. 1. Приклад блоку коефіцієнтів ДКП складової яскравості

В той же час людське око не володіє такою високою чутливістю, щоб відчути зміни цих коефіцієнтів. Тому запропоновано метод, що максимально використовує середньочастотні компоненти зображення.

Приклад блоку коефіцієнтів ДКП складової яскравості приведений на рис. 1, де НЧ – низькі частоти; СЧ – середні частоти; ВЧ – високі частоти.

Другий метод підвищення стійкості зображення використовує для вбудовування не тільки синю матрицю зображення, як це прийнято у загальновідомих методах, але також зелену та червону. Для використання даного методу рекомендується використовувати в якості контейнерів зображення із перевагою зеленого або червоного кольору і без великих однотонних ділянок.

**Розробка методу підвищення пропускної спроможності скритого каналу.**

Спираючись на результати дослідження переваг і недоліків існуючих методів вбудовування інформації було розроблено власний метод стеганографічного приховування інформації.

Суть розробленого стеганографічного методу полягає в тому, що зображення та секретна інформація піддаються попередній обробці для підвищення пропускної спроможності та стійкості стегосистеми.

Розроблений метод повинен забезпечувати надійність приховування інформації в зображеннях, вбудовування відносно великого обсягу інформації та стійкість до спотворень. Зображення має велику кількість сегментів, що забезпечить можливість для забезпечення відносно великого обсягу для вбудовування інформації.

Крок 1 – до зображення застосовується ДВП, результатом якого є розкладання зображення на чотири області: LL – низькочастотна область, і три області (LH, HL, HH) – високочастотні області.

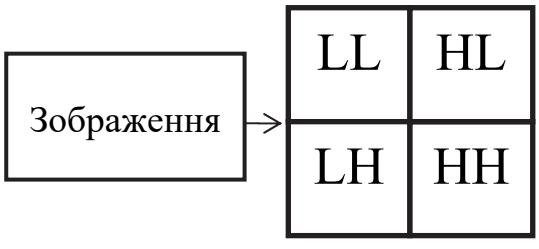


Рис. 2. Перший рівень вейвлет-перетворення

Крок 2 – обрану область (LH, HL, HH) ділять на блоки 8×8 і до кожного блоку застосовують ДКП:

$$\Omega(\upsilon,\nu)=\frac{\xi(\upsilon)\cdot\xi(\nu)}{\sqrt{2N}}\sum_{x=0}^{N-1}\sum_{y=0}^{N-1}C(x,y)\cdot\cos\left[\frac{\pi\cdot\upsilon\cdot(2x+1)}{2N}\right]\times$$

$$\times\cos\left[\frac{\pi\cdot\nu\cdot(2y+1)}{2N}\right],$$

де $C(x,y)$ – елементи оригінального і відтвореного за коефіцієнтами ДКП зображення розмірністю $N\times N$;

$x,y$ – просторові координати пікселів зображення;

$\Omega(\upsilon,\nu)$ – масив коефіцієнтів ДКП;

$\upsilon,\nu$ – координати в частотній області;

$\xi(\upsilon)=1/\sqrt{2}$, якщо $\upsilon\approx 0$, і $\xi(\upsilon)=1$, якщо $\upsilon>0$.

Крок 3 – для вбудовування було запропоновано використовувати не всі сегменти (блоки) контейнера, а тільки ті, що найбільш для цього придатні.

Придатними для вбудовування приховуваної інформації вважаються ті сегменти зображення, що одночасно задовольняють наступним двом вимогам:

– у сегменті відсутні різкі перепади яскравості;

– сегмент не є занадто монотонним.

Сегменти, що не відповідають першій вимозі, характеризуються наявністю декількох занадто великих значень НЧ коефіцієнтів ДКП, порівнянних за своєю величиною з DC-компонентою.

Для блоків, що не задовольняють другій вимозі, є характерною рівність нулеві більшості ВЧ коефіцієнтів. Таким чином, вказані особливості виступають критерієм відбраковування елементів контейнера, непридатних для заповнення. Зазначені вимоги відбраковування враховуються використанням двох порогових коефіцієнтів: $P_L$, (для першої вимоги) і $P_H$ (для другої вимоги), перевищення ($P_L$) або недосягнення ($P_H$) яких вказуватиме на те, що візуальна помітність модифікації сегмента у частотній області буде надзвичайно високою, через що останній для перенесення біта повідомлення є непридатним.

Крок 4 – з блока, приналежного СЧ області, обираються три коефіцієнти ДКП з координатами $(\upsilon_1,\nu_1)$, $(\upsilon_2,\nu_2)$ та $(\upsilon_3,\nu_3)$ відповідно.

Окрім цього, вказані коефіцієнти повинні відповідати косинус-функціям з середніми частотами, що забезпечить прихованість інформації в суттєвих для ЗСЛ областях сигналу, до того ж інформація не спотворюватиметься при JPEG-компресії з малими коефіцієнтами стиснення.

Крок 5 – якщо необхідно провести вбудовування "0", ці коефіцієнти змінюються таким чином, щоб третій коефіцієнт став менше кожного з перших двох; якщо ж потрібно приховати "1", то коефіцієнт з координатами $(\upsilon_3,\nu_3)$ робиться більшим за інші:

$$\begin{cases}(\Omega_b)_{\upsilon_3\nu_3}<(\Omega_b)_{\upsilon_1\nu_1}\\(\Omega_b)_{\upsilon_3\nu_3}<(\Omega_b)_{\upsilon_2\nu_2}\end{cases}\ \textit{при}\ M_b=0;$$

$$\begin{cases}(\Omega_b)_{\upsilon_3\nu_3} > (\Omega_b)_{\upsilon_1\nu_1} \\ (\Omega_b)_{\upsilon_3\nu_3} > (\Omega_b)_{\upsilon_2\nu_2}\end{cases} \text{ при } M_b = 1,$$

де $M_b$ – номер блоку;

$\upsilon_1\nu_1$, $\upsilon_2\nu_2$, $\upsilon_3\nu_3$ – координати коефіцієнтів ДКП;

$\Omega_b$ – матриця 8×8 коефіцієнтів розкладу.

Крок 6 – вбудовування інформації здійснюється таким чином, щоб різниця абсолютних значень коефіцієнтів ДКП перевищувала деяку позитивну величину $P$, наприклад $P = 50$, при передачі біта "0", а для передачі біта "1" ця різниця робиться меншою в порівнянні з цією ж негативною величиною $P$:

$$\begin{cases}(\Omega_b)_{\upsilon_3\nu_3} < \min\left[(\Omega_b)_{\upsilon_1\nu_1}, (\Omega_b)_{\upsilon_2\nu_2}\right] - P, \text{ при } M_b = 0; \\ (\Omega_b)_{\upsilon_3\nu_3} > \max\left[(\Omega_b)_{\upsilon_1\nu_1}, (\Omega_b)_{\upsilon_2\nu_2}\right] + P, \text{ при } M_b = 1.\end{cases}$$

Чим більше значення $P$, тим стеганосистема, створена на основі даного методу, є стійкішою до компресії та впливу завад, проте якість зображення при цьому може значно погіршуватись.

У випадку, якщо така модифікація призводить до занадто великої деградації зображення, коефіцієнти $\Omega_b$ залишають без змін, а сам блок в якості контейнера не використовується. Використання трьох коефіцієнтів ДКП замість двох і, що найголовніше, відмова від модифікації у випадку неприйнятних спотворень зображення, суттєво зменшує помітність сгеанограми.

Розроблений метод утворений шляхом інтеграції запропонованих методів підвищення стійкості, захищеності та пропускної здатності стеганографічних систем.

## Висновки

Запропоновано концепцію стеганографічного приховування даних для підвищення пропускної спроможності. Для порівняння були обрані первинні LH, HL області зображення.

Вибрані блоки за допомогою розробленого методу є стійкими до компресійних атак та вносять незначні спотворення до зображення, що дозволяє використовувати зображення для стеганографічного приховування даних.

Розроблений метод стеганографічного приховування даних за допомогою методу дискретного вейвлет-перетворення та методу Бенгама-Мемона-Ео-Юнга є стійким до відомих активних атак та стеганографічного аналізу зі сторони противника.

## Список літератури


1. Грибунин В.Г. Цифровая стеганография / В.Г. Грибунин, И.Н. Оков, И.В. Туринцев. – М.: Солон-пресс, 2018. – 248 с.
2. Efficient hierarchical graph-based video segmentation / M. Grundmann, V. Kwatra, M. Han, I. Essa // 2010 IEEE Computer Society Conference on Computer Vision and Pattern Recognition, San Francisco, California, 13-18 Jun, pp. 2141–2148.
3. Gonzalez R. Digital image processing / R. Gonzalez, K. Woods. – Tekhnosfera, 2018. – 1104 p.
4. Konakhovich G.F. Computer steganography. Theory and practice / G.F. Konakhovich, A.Yu. Puzyrenko. – Kyiv: Press, 2016. - 288 p.
5. Miano J. Formats and image compression algorithms in action / J. Miano. – Kyiv: Triumph, 2013. – 336 p.
6. Абламейко С.В. Обработка изображений: технология, методы, применение / С.В. Абламейко, Д.М. Лагуновский. – Минск: Амалфея, 2000. – 304 с.
7. Miano J. Compressed image file formats: JPEG, PNG, GIF, XBM, BMP / J. Miano. – Moscow: ACM, 1999. – 264 p.
8. Pratt W.K. Slant transform image coding / W.K. Pratt, W.H. Chen, L.R. Welch // Proc. Computer Processing in communications. – New York: Polytechnic Press, 1969. – 184 p.
9. Encoding mode selection in HEVC with the use of noise reduction / O. Stankiewicz, K. Wegner, D. Karwowski, J. Stankowski, K. Klimaszewski, T. Grajek // International Conference on Systems, Signals and Image Processing (IWSSIP). – Poznan, 2017, – P. 1-6.
10. Utility-Driven Adaptive Preprocessing for Screen Content Video Compression / S. Wang, X. Zhang, X. Liu, J. Zhang, S. Ma, W. Gao // IEEE Transactions on Multimedia. – 2017. – Vol. 19, No. 3. – P. 660-667.
11. Christophe E. Quality criteria benchmark for hiperspectral imagery / E. Christophe, D. Lager, C. Mailhes // IEEE Transactions on Geoscience and Remote Sensing. – Sept. 2005. – Vol. 43, No. 9. – P. 2103-2114.
12. A steganographic method based on the modification of regions of the image with different saturation / V. Barannik, A. Bekirov, A. Lekakh, D. Barannik // Advanced Trends in Radioelecrtronics, Telecommunications and Computer Engineering (TCSET), 14th International Conference, Lviv-Slavske, Ukraine. – 2018. – P. 542-545. https://doi.org/10.1109/TCSET.2018.8336260.
13. Detections of sustainable areas for steganographic embedding / V. Barannik, A. Alimpiev, A. Bekirov, D. Barannik, N. Barannik // 15 th IEEE East-West Design & Test Symposium (EWDTS) Novi Sad, Serbia, 2017. – P. 555-558. https://doi.org/10.1109/EWDTS.2017.8110028.
14. Methodological basis for constructing a method for compressing of transformants bit representation, based on non-equilibrium positional encoding / V.V. Barannik, Y.N. Ryabukha, V.V. Tverdokhleb, D.V. Barannik // 2017 2nd International Conference on Advanced Information and Communication Technologies (AICT). https://doi.org/10.1109/aiact.2017.8020096.

15. Баранник В.В. Основы теории структурно-комбинаторного стеганографического кодирования: монография / В.В. Баранник, Д.В. Баранник, А.Э. Бекиров. – Х.: Издательство "Лидер", 2017. – 256 с.

16. The new method of secure data transmission on the indirect steganography basis / A. Bekirov, D. Barannik, O. Frolov, O. Suprun // IEEE East-West Design & Test Symposium (EWDTS). – Yerevan, Armenia. – 2016. – P. 1-4. https://doi.org/10.1109/EWDTS.2016.7807754.

## References

1. Gribunin, V.G., Okov, I.N. and Turintsev, I.V. (2018) "*Tsifrovaya steganografiya*" [*Digital steganography*], Solon Press, Moscow, 248 p.

2. Grundmann, M., Kwatra, V., Han, M. and Essa, I. (2010), Efficient hierarchical graph-based video segmentation, *2010 IEEE Computer Society Conference on Computer Vision and Pattern Recognition*, San Francisco, California, pp. 2141-2148.

3. Gonzalez, R. and Woods, K. (2018), *Digital image processing*, Tekhnosfera, Kyiv, 1104 p.

4. Konakhovich, G.F. and Puzyrenko, A.Yu. (2016), *Computer steganography. Theory and practice*, Press, Kyiv, 288 p.

5. Miano, J. (2013), *Formats and image compression algorithms in action*, Triumph, Kyiv, 336 p.

6. Ablamejko, S.V. and Lagunovskij, D.M. (2000), "*Obrabotka izobrazhenij: tehnologija, metody, primenenie*" [*Image processing: technology. methods. application*], Amalfeja, Minsk, 303 p.

7. Miano, J. (1999), *Compressed image file formats: JPEG, PNG, GIF, XBM, BMP*, ACM, Moscow, 264 p.

8. Pratt ,W.K., Chen, W.H. and Welch, L.R. (1969), Slant transform image coding, *Computer Processing in communications*, New York, 184 p.

9. Stankiewicz, O., Wegner, K., Karwowski, D., Stankowski, J., Klimaszewski, K. and Grajek, T. (2017), Encoding mode selection in HEVC with the use of noise reduction, *International Conference on Systems, Signals and Image Processing* (IWSSIP), Poznan, pp. 1-6.

10. Wang, S., Zhang, X., Liu, X., Zhang, J., Ma, S.and Gao, W. (2017), Utility-Driven Adaptive Preprocessing for Screen Content Video Compression, *IEEE Transactions on Multimedia*, Vol. 19, No. 3, pp. 660-667.

11. Christophe, E., Lager, D. and Mailhes, C. (2005), Quality criteria benchmark for hiperspectral imagery, *IEEE Transactions on Geoscience and Remote Sensing*, Vol. 43, No 9, pp. 2103-2114.

12. Barannik, V., Bekirov, A., Lekakh, A. and Barannik, D. (2018), A steganographic method based on the modification of regions of the image with different saturation, *14th International Conference on Advanced Trends in Radioelecrtronics, Telecommunications and Computer Engineering* (TCSET). https://doi.org/10.1109/tcset.2018.8336260.

13. Barannik, V., Alimpiev, A., Bekirov, A., Barannik, D. and Barannik, N. (2017), Detections of sustainable areas for steganographic embedding, *15 th IEEE East-West Design & Test Symposium (EWDTS)*, Novi Sad, Serbia, pp. 555-558. https://doi.org/ 10.1109/EWDTS.2017.8110028.

14. Barannik, V.V., Ryabukha, Y.N., Tverdokhleb, V.V. and Barannik, D.V. (2017), Methodological basis for constructing a method for compressing of transformants bit representation, based on non-equilibrium positional encoding, *2nd International Conference on Advanced Information and Communication Technologies (AICT).* https://doi.org/10.1109/aiact.2017.8020096.

15. Barannik, V.V., Barannik, D.V. and Bekirov, A.E. (2017), "*Osnovyi teorii strukturno-kombinatornogo steganograficheskogo kodirovaniya: monografiya*" [*Fundamentals of the theory of structurally combinatorial steganographic coding: monograph*], Leader, Kharkiv, 256 p.

16. Bekirov, A., Barannik, D., Frolov, O. and Suprun, O. (2016), The new method of secure data transmission on the indirect steganography basis, *IEEE East-West Design & Test Symposium (EWDTS)*. https://doi.org/10.1109/ewdts.2016.7807754.

*Надійшла до редколегії 30.08.2019*
*Схвалена до друку 15.10.2019*

***Відомості про авторів:***

**Тупиця Іван Михайлович**
викладач Харківського національного університету Повітряних Сил ім. І. Кожедуба, Харків, Україна
https://orcid.org/0000-0001-6806-4914

**Димчук Вікторія Володимирівна**
курсант Харківського національного університету Повітряних Сил ім. І. Кожедуба, Харків, Україна
https://orcid.org/0000-0002-8290-303X

**Чуянов Кирило Вадимович**
курсант Харківського національного університету Повітряних Сил ім. І. Кожедуба, Харків, Україна
https://orcid.org/0000-0003-3105-5381

***Information about the authors:***

**Ivan Tupitsya**
Instructor of Ivan Kozhedub Kharkiv National Air Force University, Kharkiv, Ukraine
https://orcid.org/0000-0001-6806-4914

**Viktoria Dymchuk**
Cadet of Ivan Kozhedub Kharkiv National Air Force University, Kharkiv, Ukraine
https://orcid.org/0000-0002-8290-303X

**Kyrylo Chuyanov**
Cadet of Ivan Kozhedub Kharkiv National Air Force University, Kharkiv, Ukraine
https://orcid.org/0000-0003-3105-5381

**Кодацький Микола Миколайович**
курсант Харківського національного
університету Повітряних Сил ім. І. Кожедуба,
Харків, Україна
https://orcid.org/0000-0002-2779-2103

**Mikola Kodatsky**
Cadet of Ivan Kozhedub
Kharkiv National Air Force University,
Kharkiv, Ukraine
https://orcid.org/0000-0002-2779-2103

## МЕТОД ПОВЫШЕНИЯ ПРОПУСКНОЙ СПОСОБНОСТИ СКРЫТОГО КАНАЛА В ИНФОКОМУНИКАЦИОННЫХ СИСТЕМАХ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

И.М. Тупица, В.В. Димчук, К.В. Чуянов, Н.Н. Кодацкий

*В статье рассматриваются вопросы, связанные с разработкой метода повышения пропускной способности скрытого канала для информационных технологий обработки и передачи видеоинформационных ресурсов. Развитие систем, использующих изображения и видео для передачи данных, заставляет внедрять методы цифровой стеганографии для защиты данных. В результате анализа установлено, что методы цифровой стеганографии имеют ряд недостатков: низкая устойчивость к атакам, низкая пропускная способность, небольшой объем стеганографической емкости и являются неустойчивыми при передаче изображений и активных атаках противника, возможна потеря данных. С целью стеганографического сокрытия данных был разработан метод, который реализуется путем интеграции методов дискретного вейвлет-преобразования и Бенгама-Мемон-Эо-Юнга. Разработанный метод является устойчивым к известным активным атакам и стеганографическому анализу со стороны противника.*

***Ключевые слова:*** *цифровая стеганография, пропускная способность, атака, дискретное вейвлет-преобразование.*

## METHOD FOR INCREASING HIDDEN CHANNEL CAPACITY IN INFOCOMMUNICATION SYSTEMS FOR SPECIAL PURPOSE

I. Tupitsya, V. Dymchuk, K. Chuyanov, M. Kodatsky

*The article discusses issues related to the development of a method for increasing the throughput of a covert channel for information processing and transmission of video information resources. The development of systems that use images and video for data transmission forces the introduction of digital steganography methods to protect data. The purpose of the work is to find new approaches to improve the efficiency of hidden information transmission systems in telecommunication systems based on the steganographic method with high rates of stability and throughput. The task of scientific work is to study the methods of digital steganography. The following methods have been analyzed and investigated: the discrete wavelet - transform method, the Bengh - Memon - Eo - Jung method, the least significant bit method, the Koch - Zhao method. As a result of the analysis, it was found that digital steganography methods have several disadvantages: low resistance to attacks, low bandwidth, a small amount of steganographic capacity and are unstable when transmitting images and active enemy attacks, data loss is possible. In order to steganographically hide data, a method has been developed that is implemented by integrating discrete wavelet transform and Bengam-Memon-Eo-Young methods. The concept of steganographic data hiding to increase throughput is proposed. For comparison, the primary areas of the image were selected. Using the developed method, selected blocks are resistant to compression attacks and introduce slight distortions into the image, which allows using images for steganographic data hiding. The developed method is resistant to known active attacks and steganographic analysis by the enemy.*

***Keywords*****:** *digital steganography, bandwidth, attack, discrete wavelet – conversion.*