УДК 004.056.5:621.391 DOI: 10.26565/2519-2310-2019-4-01

ПСЕВДОВИПАДКОВІ ДИСКРЕТНІ ПОСЛІДОВНОСТІ ДЛЯ СТЕГАНОСИСТЕМ З ВИКОРИСТАННЯМ ТЕХНОЛОГІЇ ПРЯМОГО РОЗШИРЕННЯ СПЕКТРА

Олексій Смірнов[1], Анна Арищенко[2], Євгеній Деменко[2], Олександр Онікійчук[2], Олександр Кузнецов[2]

[1] - Центральний український НТУ, Кропивницький, Україна
[2] - Харківський національний університет імені В.Н. Каразіна, майдан Свободи 4, Харків, 61022, Україна
dr.smirnovoa@gmail.com, annaarischenko@gmail.com, demenjay@gmail.com, onik4524a@gmail.com, kuznetsov@karazin.ua

Рецензент: Микола Карпінський, д.т.н., проф., університет Бельсько-Бяла, Бельсько-Бяла, Польща.
mkarpinski@ath.bielsko.pl

Надійшло: Січень 2020.

Анотація. *В статті розглядаються псевдовипадкові дискретні послідовності (сигнали), які використовуються для стеганографічного приховування інформаційних повідомлень у контейнерах-зображеннях. Для приховування застосовується технологія прямого розширення спектра, суть якої полягає в модуляції інформаційних даних довгими псевдовипадковими (шумовими) послідовностями. Повідомлення набувають вигляду шуму, через що виявити таку передачу вкрай складно. В роботі досліджуються різні способи формування дискретних сигналів і оцінюється інтенсивність помилок при відновленні повідомлень. Виявлено, що спосіб формування псевдовипадкових послідовностей впливає на інтенсивність помилок, тому в роботі обґрунтовується вибір найбільш придатних сигналів. Крім того, оцінюється викривлення контейнера-зображення в результаті приховування даних. Стаття містить переважно результати експериментальних досліджень, які можуть бути корисними при обґрунтуванні різних варіантів побудови стеганографічних систем з прямим розширенням спектра.*

Ключові слова: *приховування інформації; стеганографія; технологія прямого розширення спектру; псевдовипадкова послідовність; розширюючі сигнали.*

1 Вступ

Для приховування даних в контейнерах-зображеннях використовують різні стеганографічні методи [1-4]. Найбільш цікавим підходом є застосування технології прямого розширення спектру [5-17]. Технологія прямого розширення спектра традиційно використовується в системах радіозв'язку з множинним доступом [18-21]. Вона заснована на модуляції інформаційних повідомлень так званими розширюючими сигналами - довгими псевдовипадковими послідовностями, що мають хаотичний, шумоподібний вид. У цьому випадку передане повідомлення стає подібно шуму і його дуже складно розпізнати. Крім того, застосовані методи кореляційного прийому складних шумоподібних сигналів дозволяють виправляти помилки, підвищуючи тим самим завадостійкість системи зв'язку.

У роботах [5-17] технологія прямого розширення спектра частот застосовується для приховування інформаційних повідомлень у цифрових контейнерах-зображеннях. Наприклад, в [5-11] пропонувалося використовувати нелінійну модуляцію псевдовипадковими послідовностями, елементи яких розподілені за нормальним законом з нульовим середнім і одиничним середньоквадратичним відхиленням. Дійсно, інтерпретуючи зображення як шум в каналі зв'язку (КЗ), вдається приховати інформаційні повідомлення при прийнятному рівні внесених викривлень в контейнер.

Ціллю даної статті є дослідження різних варіантів формування розширюючих сигналів, а також їх впливу на якісні характеристики стеганосистеми. Зокрема, в роботі оцінюється достовірність переданих даних, шляхом оцінювання інтенсивності бітових помилок (*BER*) у відновлених повідомленнях. Крім того, оцінюється величина внесених викривлень в контейнер-зображення. Для цього розраховується середньоквадратична помилка (*MSE*), між вихідним зображенням і тим, яке отримано після приховування в ньому інформаційного повідомлення. Розглянуті характеристики (*BER* і *MSE*) дозволяють порівняти різні варіанти формування розширюючих спектр сигналів. У роботі показано, що зміна правил формування сигналів може істотно впливати на BER.

Звичайно, в системах радіозв'язку з прямим розширенням спектру природний шум у КЗ не є корельований із розширюючими послідовностями. Однак, у разі приховування інформації в цифрові зображення це може бути не так. Найближчі (*сусідні*) пікселі реалістичних зображень досить сильно корельовані і цей зв'язок може істотно порушити базові припущення, що обумовлюють правильне відновлення прихованих інформаційних даних (*стеганоконтенту*). У цій статті досліджується декілька варіантів формування розширюючих сигналів і обґрунтовується вибір кращої альтернативи.

2 Технологія прямого розширення спектру в стеганографії

Передача даних у системах радіозв'язку з використанням технології прямого розширення спектру може бути спрощено представлена у вигляді співвідношення (1):

$$N = I + P\sum_{i=1}^{k} b_i\varphi_i, \tag{1}$$

де кожен інформаційний біт $b_i \in \{-1,1\}$ множиться на розширюючу псевдовипадкову послідовність φ_i із множини (ансамблю) слабокорелюючих дискретних сигналів:

$$\forall \varphi_i \in \varphi = \{\varphi_0, \varphi_1, ..., \varphi_{M-1}\}, \tag{1а}$$

$$\forall i \neq j : \rho(\varphi_i, \varphi_j) \approx 0, \tag{1б}$$

- P - коефіцієнт посилення потужності дискретних сигналів;
- k - число бітів інформаційного повідомлення, які передаються одночасно в каналі зв'язку (в системах кодового розподілу каналів ця величина може характеризувати абонентську ємність множинного доступу);
- I - природний шум в КЗ;
- $\rho(\varphi_i, \varphi_j)$ - коефіцієнт взаємної кореляції послідовностей φ_i та φ_j;
- N - отриманий на приймальній стороні сигнал (*адитивна суміш корисного сигналу та шуму*).

Відновлення інформації здійснюється за допомогою кореляційного прийому. Для цього обчислюється коефіцієнт кореляції (*скалярний добуток векторів*):

$$\rho\left(N, \varphi_j\right) = I\varphi_j + \varphi_j P\sum_{i=1}^{k} b_i\varphi_i \cdot \tag{1в}$$

У системах зв'язку природний шум і шумовий сигнал φ_i статистично незалежні (*некорельовані*), тобто $\rho\left(I, \varphi_j\right) = I\varphi_j \approx 0$. Різні шумові сигнали також некорельовані один з одним, отже $\forall j \neq i : \varphi_j\varphi_i \approx 0$. Тоді $\rho\left(N, \varphi_j\right) \approx Pb_j\varphi_j\varphi_j$ і значення b_j можна визначити за знаком $\rho\left(N, \varphi_j\right)$:

$$b_j = sign\left[\rho\left(N, \varphi_j\right)\right]. \tag{2}$$

Для приховування інформаційного повідомлення в контейнері-зображенні використовуються наступні припущення [5-11]. При цьому, цифрове зображення інтерпретується, як шум в КЗ, при цьому ми припускаємо, що $\rho\left(I, \varphi_j\right) = I\varphi_j \approx 0 \cdot$

Інформаційні біти модулюються розширюючими послідовностями: $\sum_{i=1}^{k} b_i\varphi_i$, після чого, так само як і в (1), посилений результат додається до контейнера-зображення.

Для відновлення інформаційних бітів, також, використовується правило (2).

Як і раніше, вважаємо $\forall j \neq i : \varphi_j \varphi_i \approx 0$. Однак припущення $\rho\left(I, \varphi_j\right) = I\varphi_j \approx 0$ може не виконуватися. Дійсно, окремі пікселі реалістичних зображень сильно корельовані. В цьому випадку результат $\rho\left(I, \varphi_j\right) = I\varphi_j$ залежить від статистичних властивостей розширюючих послідовностей, тобто від способу формування множини $\varphi = \{\varphi_0, \varphi_1, ..., \varphi_{M-1}\}$.

В цій статті розглядаються різні способи формування дискретних сигналів і досліджується ефективність їх використання для приховування повідомлення в контейнерах-зображеннях. Оцінюється інтенсивність бітових помилок (BER) при відновленні даних за правилом (2).

Показник BER – кількість бітових помилок N_{error} розділених на загальну кількість переданих N_{total} [23]:

$$BER = \frac{N_{error}}{N_{total}}. \tag{3}$$

Отже BER - критерій якості роботи, який виражається у відсотках [23]. В даній статті він оцінюється в абсолютних величинах, тобто безпосередньо по формулі (3).

В проведених дослідженнях BER оцінювалося без використання завадостійкого кодування. Цей випадок також розглядається в інших роботах, наприклад, в таблиці 2 з [8] наведено схожі результати.

Для оцінки викривлень контейнера-зображення використовують показник MSE [23-25]. Для монохромного $m \times n$ зображення I значення MSE визначають за формулою (4):

$$MSE = \frac{1}{mn} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} [I_{i,j} - N_{i,j}]^2, \tag{4}$$

де N - викривлене помилками наближення контейнера-зображення (*далі - контейнера*), як, наприклад, в (1).

В якості вихідних даних використовувалися різні 256×256 зображення (по аналогії з роботами [7-8, 10-11]). Наведені нижче результати становлять усереднені значення, які отримані за кількома різними зображеннями.

3 Результати досліджень

Розглянемо декілька варіантів формування розширюючих послідовностей в (1). Для кожного випадку будуть оцінені BER та MSE. Дані значення характеризують помилки у відновленому повідомленні та викривлення, що вносяться у контейнер.

Розглянемо декілька варіантів формування розширюючих послідовностей в (1). Для кожного випадку будуть оцінені BER та MSE. Дані значення характеризують помилки у відновленому повідомленні та викривлення, що вносяться у контейнер-зображення.

3.1 Нелінійні послідовності зі стандартним нормальним розподілом

Перший випадок, який буде розглянуто, описаний в роботах [7-8, 10-11], де пропонується формувати кожну розширюючу послідовність із використання відношень (5, 6):

$$\left(\varphi_i\right)_j = \begin{cases} \Phi^{-1}((u_i)_j), b_j = -1; \\ \Phi^{-1}((u_i')_j), b_i = 1, \end{cases} \tag{5}$$

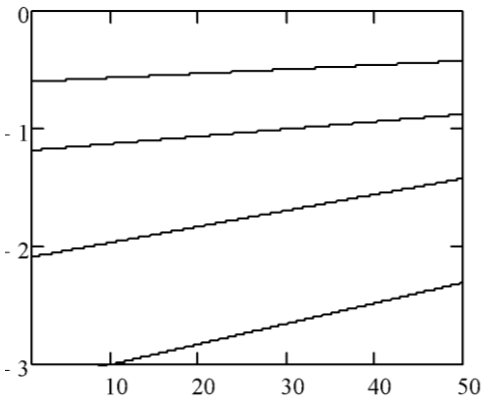
де

$$(u_i')_j = \begin{cases} (u_i)_j + 0.5, u_i < 0.5; \\ (u_i)_j - 0.5, u_i \geq 0.5, \end{cases} \tag{6}$$

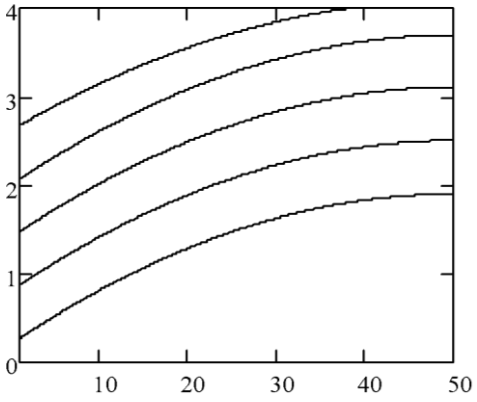
- $(u_i)_j$ - рівномірно розподілена на інтервалі (0,1) випадкова величина;

- Φ^{-1} представляє собою зворотну кумулятивну функцію розподілу для стандартної гаусової випадкової величини.

Отримані результати для різних P (для дискретних послідовностей із [7, 8, 10, 11]), наведені на рис. 1.



а) BER(k), P = 8, 16, 32, 64

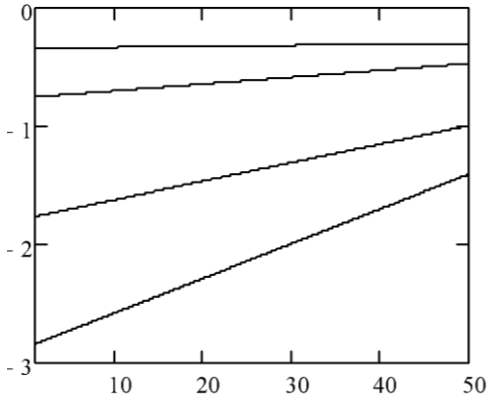


б) MSE(k), P = 1, 2, 4, 8, 16

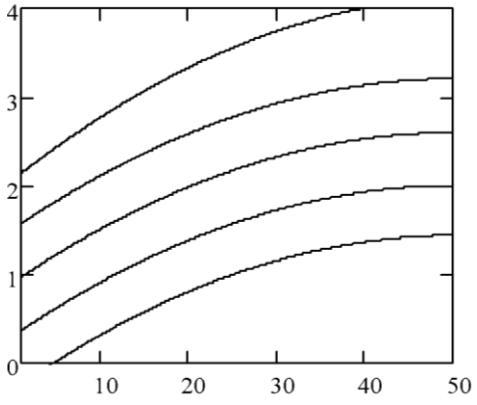
Рис. 1 – Емпіричні залежності BER(k) та MSE(k)

3.2 Дискретні послідовності з рівномірним на інтервалі (-1,1) розподілом

В цій роботі було досліджено ще кілька способів формування розширюючих послідовностей. Як альтернатива стандартному нормальному розподілу було реалізовано інший спосіб формування дискретних послідовностей, коли їхні елементи розподілені за рівномірним на інтервалі (-1,1) законом. Результати експериментальних досліджень, для дискретних послідовностей з рівномірно розподіленими на інтервалі (-1,1) значеннями, наведені на рис. 2.



а) BER(k), P = 8, 16, 32, 64



б) MSE(k), P = 1, 2, 4, 8, 16

Рис. 2 – Емпіричні залежності BER(k) та MSE(k)
(з рівномірно розподіленими на інтервалі (-1,1) значеннями)

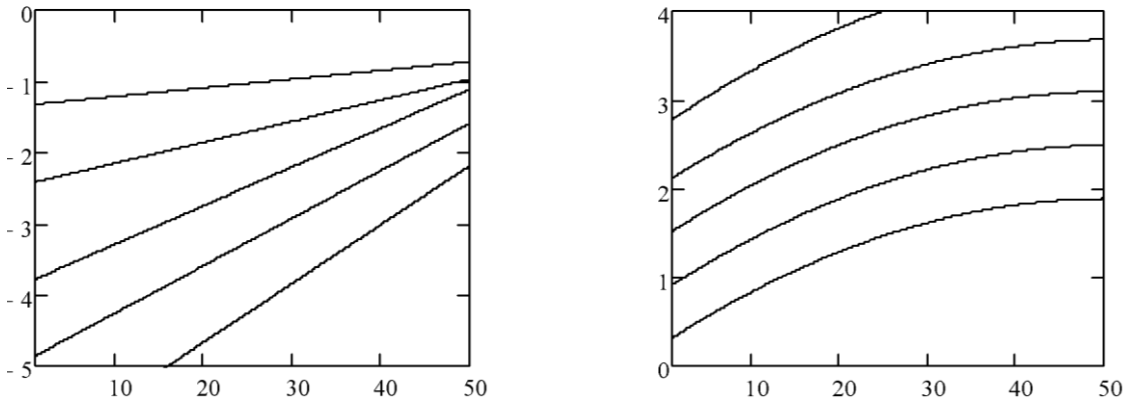
3.3 Ортогональні дискретні сигнали Уолша-Адамара

Ще один спосіб формування множини $\varphi = \{\varphi_0, \varphi_1, \ldots, \varphi_{M-1}\}$, який було досліджено, полягав у використанні матриць Адамара. Ці матриці формуються за рекурентним правилом (7):

$$H_{2^i} = \begin{bmatrix} H_{2^{i-1}} & H_{2^{i-1}} \\ H_{2^{i-1}} & -H_{2^{i-1}} \end{bmatrix}, \; H_1 = [1] \qquad (7)$$

При цьому, рядки (або стовбці) матриць H_{2^i} взаємно ортогональні, тобто їхній скалярний добуток дорівнює нулю. Множину дискретних сигналів $\varphi = \{\varphi_0, \varphi_1, \ldots, \varphi_{M-1}\}$, складену з таких рядків (або стовпців), називають послідовностями Уолша-Адамара [22].

Результати експериментальних досліджень BER і MSE для випадку для дискретних послідовностей (*сигналів*) Уолша-Адамара наведені на рис. 3.



а) BER(k), P = 1, 2, 4, 8, 16 *б) MSE(k), P = 1, 2, 4, 8, 16*

Рис. 3 – Емпіричні залежності BER(k) та MSE(k)
(для сигналів Уолша-Адамара)

4 Результати та висновки

За результатами проведених експериментальних досліджень можна побачити, що всі розглянуті способи генерації дискретних сигналів практично еквівалентні по викривленню зображення-контейнера. Це пояснюється близьким діапазоном можливих значень елементів послідовностей, та схожим способом приховування інформації. При цьому, невелику перевагу мають сигнали з нелінійним правилом модуляції, які були запропоновані в роботах [7-8 та 10-11]. Найгірше, за критерієм MSE, виглядають ортогональні дискретні сигнали Уолша-Адамара (*але цей програш невеликий і практично непомітний на логарифмічній шкалі*).

За критерієм мінімізації BER перші два способи формування дискретних сигналів практично однакові. Навіть при високому коефіцієнті посилення P ці методи формування розширюючих послідовностей не дають можливості отримати малі величини BER. Наприклад, навіть при $P = 64$ інтенсивність помилки приблизно дорівнює 10^{-3} і вище, що передбачає обов'язкове використання завадостійких кодів. Невелику перевагу серед перших двох способів мають нелінійні послідовності, що розглянуті в роботах [7-8 та 10-11]. Однак найбільш ефективним способом зі зниженням BER, є використання дискретних сигналів Уолша-Адамара.

Із діаграм, які наведено на рис. 3 слідує, що навіть при $P = 16$ вже досягаються низькі значення BER, що, приблизно, дорівнюють 10^{-5} та нижче. Це відкриває досить широкі можливості стосовно практичної побудови стеганографічних систем приховування інформації в контейнерах-зображеннях різного типу.

Багатообіцяючим напрямком подальших досліджень є розробка адаптивного алгоритму формування розширюючих псевдовипадкових послідовностей. Наприклад, якщо правило формування дискретних сигналів із множини $\varphi = \{\varphi_0, \varphi_1, \ldots, \varphi_{M-1}\}$ буде враховувати статистичні властивості зображення-контейнера, то інтенсивність помилок BER можна істотно знизити, та навидь домогтися безпомилкового відновлення інформації. В цьому сенсі перспективним напрямом слід вважати використання нових класів псевдовипадкових послідовностей, які запропоновані в роботах [26-30].

Посилання

[1] “Digital Watermarking and Steganography,” 2008. doi:10.1016/b978-0-12-372585-1.x5001-3.

[2] F. Y. Shin, “Digital Watermarking and Steganography,” Dec. 2017. doi:10.1201/9781315219783.

[3] N. F. Johnson and S. Jajodia, "Exploring steganography: Seeing the unseen," in Computer, vol. 31, no. 2, pp. 26-34, Feb. 1998. doi: 10.1109/MC.1998.4655281 .

[4] I. V. S. Manoj, “Cryptography and Steganography,” International Journal of Computer Applications, vol. 1, no. 12, pp. 63–68, Feb. 2010. doi:10.5120/257-414.

[5] A. Z. Tirkel, C. F. Osborne and R. G. Van Schyndel, "Image watermarking-a spread spectrum application," Proceedings of ISSSTA'95 International Symposium on Spread Spectrum Techniques and Applications, Mainz, Germany, 1996, pp. 785-789 vol.2. doi: 10.1109/ISSSTA.1996.563231.

[6] J. R. Smith and B. O. Comiskey, “Modulation and information hiding in images,” Lecture Notes in Computer Science, pp. 207–226, 1996. doi:10.1007/3-540-61996-8_42.

[7] L. M. Marvel, C. G. Boncelet, R. Jr., and Charles T., “Methodology of Spread-Spectrum Image Steganography,” Jun. 1998. doi:10.21236/ada349102.

[8] L. M. Marvel, C. G. Boncelet and C. T. Retter, "Spread spectrum image steganography," in IEEE Transactions on Image Processing, vol. 8, no. 8, pp. 1075-1083, Aug. 1999. doi: 10.1109/83.777088.

[9] M. Kutter, “Performance Improvement of Spread Spectrum Based Image Watermarking Schemes through M-ary Modulation,” Lecture Notes in Computer Science, pp. 237–252, 2000. doi:10.1007/10719724_17.

[10] F. S. Brundick and L. M. Marvel, “Implementation of Spread Spectrum Image Steganography,” Mar. 2001. doi:10.21236/ada392155.

[11] Patent No.: US 6,557,103 B1, Int.Cl. G06F 11/30. Charles G. Boncelet, Jr., Lisa M. Marvel, Charles T. Retter. Spread Spectrum Image Steganography. Patent No.: US 6,557,103 B1, Int.Cl. G06F 11/30. – № 09/257,136; Filed Feb. 11, 1999; Date of Patent Apr. 29, 2003

[12] Fan Zhang, Bin Xu and Xinhong Zhang, "Digital image watermarking algorithm based on CDMA spread spectrum," 2006 12th International Multi-Media Modelling Conference, Beijing, 2006, pp. 4 pp.-. doi: 10.1109/MMMC.2006.1651359.

[13] T. T. Nguyen and D. Taubman, "Optimal linear detector for spread spectrum based multidimensional signal watermarking," 2009 16th IEEE International Conference on Image Processing (ICIP), Cairo, 2009, pp. 113-116. doi: 10.1109/ICIP.2009.5414121.

[14] E. Nezhadarya, Z. J. Wang and R. K. Ward, "Image quality monitoring using spread spectrum watermarking," 2009 16th IEEE International Conference on Image Processing (ICIP), Cairo, 2009, pp. 2233-2236. doi: 10.1109/ICIP.2009.5413955.

[15] S. Ghosh, P. Ray, S. P. Maity and H. Rahaman, "Spread Spectrum Image Watermarking with Digital Design," 2009 IEEE International Advance Computing Conference, Patiala, 2009, pp. 868-873. doi: 10.1109/IADCC.2009.4809129.

[16] H. O. Altun, A. Orsdemir, G. Sharma and M. F. Bocko, "Optimal Spread Spectrum Watermark Embedding via a Multistep Feasibility Formulation," in IEEE Transactions on Image Processing, vol. 18, no. 2, pp. 371-387, Feb. 2009. doi: 10.1109/TIP.2008.2008222.

[17] A. Samčović and M. Milovanović, "Robust digital image watermarking based on wavelet transform and spread spectrum techniques," 2015 23rd Telecommunications Forum Telfor (TELFOR), Belgrade, 2015, pp. 811-814. doi: 10.1109/TELFOR.2015.7377589.

[18] V. P. Ipatov, “Spread Spectrum and CDMA,” Mar. 2005. doi:10.1002/0470091800.

[19] “Introduction to CDMA Wireless Communications,” 2007. doi:10.1016/b978-0-7506-5252-0.x5001-7.

[20] “The Generalized CDMA,” CDMA: Access and Switching, pp. 1–28. doi:10.1002/0470841699.

[21] S. Hara and R. Prasad, "DS-CDMA, MC-CDMA and MT-CDMA for mobile multi-media communications," Proceedings of Vehicular Technology Conference - VTC, Atlanta, GA, USA, 1996, pp. 1106-1110 vol.2. doi: 10.1109/VETEC.1996.501483.

[22] S. S. Agaian, H. G. Sarukhanyan, K. O. Egiazarian, and J. Astola, “Hadamard Transforms,” Aug. 2011. doi:10.1117/3.890094.

[23] “Probability Theory of Bit Error Rate,” Optical Bit Error Rate, 2009. doi:10.1109/9780470545430.ch7.

[24] J. Korhonen and J. You, "Peak signal-to-noise ratio revisited: Is simple beautiful?," 2012 Fourth International Workshop on Quality of Multimedia Experience, Yarra Valley, VIC, 2012, pp. 37-38. doi: 10.1109/QoMEX.2012.6263880

[25] “Data Compression,” 2007. doi:10.1007/978-1-84628-603-2.

[26] Yu.V. Stasev, A.A. Kuznetsov, A.M. Nosik. “Formation of pseudorandom sequences with improved autocorrelation properties.” Cybernetics and Systems Analysis, vol. 43, Issue 1, pp. 1-11, January 2007. DOI: 10.1007/s10559-007-0021-2

[27] N.I.Naumenko, Yu.V.Stasev, A.A.Kuznetsov. “Methods of synthesis of signals with prescribed properties.” Cybernetics and Systems Analysis, vol. 43, Issue 3, pp. 321-326, May 2007. DOI: 10.1007/s10559-007-0052-8

[28] O.Karpenko, A.Kuznetsov, V.Sai, Yu.Stasev. “Discrete Signals with Multi-Level Correlation Function.” Telecommunications and Radio Engineering, vol. 71, 2012 Issue 1. pp 91-98. DOI: 10.1615/TelecomRadEng.v71.i1.100

[29] A. Kuznetsov, S. Kavun, V. Panchenko, D. Prokopovych-Tkachenko, F. Kurinniy and V. Shoiko, "Periodic Properties of Cryptographically Strong Pseudorandom Sequences," 2018 International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T), Kharkiv, Ukraine, 2018, pp. 129-134. doi: 10.1109/INFOCOMMST.2018.8632021

[30] A. Kuznetsov, O. Smirnov, D. Kovalchuk, A. Averchev, M. Pastukhov and K. Kuznetsova, "Formation of Pseudorandom Sequences with Special Correlation Properties," 2019 3rd International Conference on Advanced Information and Communications Technologies (AICT), Lviv, Ukraine, 2019, pp. 395-399. doi: 10.1109/AIACT.2019.8847861

Reviewer: Mikołaj Karpiński, Dr. of Sciences (Eng.), Full Prof., University of Bielsko-Biala, Bielsko-Biala, Poland.
E-mail: mkarpinski@ath.bielsko.pl

Received: January 2020.

Authors:
Oleksii Smirnov, Central Ukrainian National Technical University, Cybersecurity & Software Academic Department, Kropivnitskiy, Ukraine. E-mail: dr.smirnovoa@gmail.com
Anna Arischenko, computer science student, V.N. Karazin Kharkiv National University, Ukraine.
E-mail: annaarischenko@gmail.com
Eugene Demenko, computer science student, V.N. Karazin Kharkiv National University, Ukraine.
E-mail: demenjay@gmail.com
Alexander Onikiychuk, computer science student, V.N. Karazin Kharkiv National University, Ukraine.
E-mail: onik4524a@gmail.com
Alexandr Kuznetsov, V. N. Karazin Kharkiv National University, Department of information systems and technologies security, Kharkiv, Ukraine. E-mail: kuznetsov@karazin.ua

Pseudorandom Sequences for Spread Spectrum Image Steganography.

Abstract. We consider pseudorandom sequences (signals), which are used for information-hiding in cover images. Spread spectrum image steganography is used for the hiding, the essence of which is modulating information data with long pseudorandom (noise) sequences. Messages take the form of noise, and it is extremely difficult to detect such transmission. We investigate different ways of discrete signals generation and estimate the error rate in message restoration. It appears, the way of discrete signals generation influences on the error rate and we prove the choice of the most suitable signals. Moreover, we estimate distortions of the cover image as a result of data-hiding. The article mainly contains the results of experimental researches, which can be useful in justifying various ways of building direct spread spectrum steganographic systems.

Keywords: Data-hiding; Steganography; Spread spectrum image steganography; Pseudorandom sequences; Spreading sequences.

Рецензент: Николай Карпинский, д.т.н., проф., Университет Бельсько-Бяла, ул. Виллова 2, 43-309 Бельсько-Бяла, Польша.
E-mail: mkarpinski@ath.bielsko.pl

Поступила: Январь 2020.

Авторы:
Алексей Смирнов, каф. кибербезопасности и программного обеспечения, Центральный украинский национальный технический университет, Кропивницкий, Украина.
E-mail: dr.smirnovoa@gmail.com
Анна Арищенко, студент факультета компьютерных наук, ХНУ имени В. Н. Каразина, Харьков, Украина.
E-mail: annaarischenko@gmail.com
Евгений Деменко, студент факультета компьютерных наук, ХНУ имени В. Н. Каразина, Харьков, Украина.
E-mail: demenjay@gmail.com
Александр Оникийчук, студент факультета компьютерных наук, ХНУ имени В. Н. Каразина, Харьков, Украина.
E-mail: onik4524a@gmail.com
Александр Кузнецов, д.т.н., проф., каф. безопасности информационных систем и технологий, Харьковский национальный университет имени В. Н. Каразина, Харьков, Украина.
E-mail: kuznetsov@karazin.ua

Псевдослучайные дискретные последовательности для сокрытия данных в контейнерах-изображениях с использованием технологии прямого расширения спектра.

Аннотация. В статье рассматриваются псевдослучайные дискретные последовательности (сигналы), которые используются для стеганографического сокрытия информационных сообщений в контейнерах-изображениях. Для сокрытия применяется технология прямого расширения спектра, суть которой состоит в моделировании информационных данных длинными псевдослучайными (шумовыми) последовательностями. Сообщения приобретают вид шума, и обнаружить такую передачу крайне сложно. В работе исследуются различные способы формирования дискретных сигналов, и оценивается интенсивность ошибок при восстановлении сообщений. Оказывается, способ формирования псевдослучайных последовательностей влияет на интенсивность ошибок, а также в работе обосновывается выбор наиболее подходящих сигналов. Кроме того, оцениваются искажения контейнера-изображения в результате сокрытия данных. В статье содержатся преимущественно результаты экспериментальных исследований, которые могут быть полезны при обосновании различных вариантов построения стеганографических систем с прямым расширением спектра.

Ключевые слова: сокрытие информации; стеганография; технология прямого расширения спектра; псевдослучайная последовательность; расширяющие сигналы.