УДК 004.056.5:621.391 DOI: 10.26565/2519-2310-2019-4-04

ФОРМУВАННЯ ПСЕВДОВИПАДКОВИХ ПОСЛІДОВНОСТЕЙ ДЛЯ ПРИХОВУВАННЯ ДАНИХ В ЗОБРАЖЕННЯХ

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

[1] - Харківський національний університет імені В.Н. Каразіна, Харків, Україна
[2] - Центральний український НТУ, Кропивницький, Україна
demenjay@gmail.com, onik4524a@gmail.com, annaarischenko@gmail.com, lusyag23@gmail.com, dr.smirnovoa@gmail.com

Рецензент: В'ячеслав Калашников, д.ф.-м.н., проф., Технологічний університет Монтеррея, Монтеррей, 64849, Мексика
kalash@itesm.mx

Надійшло: Січень 2020.

Анотація: *У статті розглядаються способи приховування даних в цифрових зображеннях з використанням псевдовипадкових послідовностей і технології прямого розширення спектра. Пропонується новий спосіб формування псевдовипадкових послідовностей, який враховує статистичні властивості контейнерів-зображень. Це дозволяє домогтися низької кореляції, що забезпечує надійне і безпечне приховування інформації в цифрових зображеннях. Результати експериментальних досліджень показують, що інтенсивність бітових помилок в відновлених повідомленнях істотно знижена. При цьому викривлення контейнерів-зображень залишаються на колишньому рівні.*

Ключові слова: *стеганографія; приховування даних; цифрові зображення; псевдовипадкова послідовність; технологія прямого розширення спектра.*

1 Вступ

Для приховування інформації в цифрових контейнерах-зображеннях в роботах [1-7] запропоновано використовувати псевдовипадкові послідовності та технологію прямого розширення спектра частот. Ця технологія традиційно використовується в системах радіозв'язку з множинним доступом [9-11]. Псевдовипадкові послідовності, які застосовуються, є слабокорельованими один з одним. Вони можуть бути співставлені різними абонентськими каналами і це дозволяє істотно підвищити ємність множинного доступу, що здешевлює послуги зв'язку. Використовуючи кореляційний прийом, можна виправляти помилки, які виникають, тим самим підвищуючи прихованість зв'язку. Крім того, застосування довгих псевдовипадкових послідовностей дозволяє організувати зв'язок при потужності переданих сигналів нижче рівня природних шумів, що забезпечує екологічність зв'язку [9-11].

Всі ці переваги можна використовувати і в інших додатках, наприклад, в цифровій стеганографії. Так в роботах [12-21] пропонується інтерпретувати зображення-контейнери, як шум в каналах зв'язку. Тоді передача даних по каналу зв'язку (КЗ) з шумами представляється як завдання приховування інформаційних повідомлень в зображеннях-контейнерах (*далі контейнерах*). При цьому завадостійкість інтерпретується як стійкість до помилок в відновлених повідомленнях, а абонентська ємність - як пропускна здатність стеганосистеми.

Слід зазначити, що запропоновані в роботах [12-21] методи приховування даних мають певні недоліки. Наприклад, базове припущення про статистичні властивості контейнера часто не виконується. Дійсно, реалістичні зображення володіють високою природною надмірністю, їхні окремі пікселі сильно корельовано між собою, тобто цифрове зображення статистично не подібно до природного шуму в КЗ. Практично це означає можливість кореляції застосовуваних псевдовипадкових послідовностей (ПВП) і контейнерів. У цьому випадку відновлення інформаційних повідомлень на приймальній стороні часто відбувається з великим числом помилок. Наприклад, в роботі [14] показано, що інтенсивність бітових помилок (*Bit Error Rate - BER*) в відновлених повідомленнях від 10% до 30% і ніколи не опускається нижче 10% (*навіть при дуже високій потужності дискретних сигналів - псевдовипадкових послідовностей*). Це змушує використовувати досить складні технології корекції помилок, засновані на внесенні додаткової надмірності [15].

Мета даної роботи полягає в розгляді та дослідженні іншого способу зниження помилок в повідомленнях що відновлюються. Так, замість корекції помилок пропонується використовувати спеціально сформовані ПВП, т.зв. адаптивну генерацію, тобто процедуру, яка при формуванні послідовностей враховує статистичні властивості контейнерів. Проведені експериментальні дослідження підтвердили успішність зазначеного підходу, адже вдається істотно знизити інтенсивність помилок в відновлених повідомленнях (*стеганоконтенті*). При цьому викривлення контейнерів залишаються на колишньому рівні.

2 Технологія прямого розширення спектру в стеганографії

У роботах [12-21] розглянуті базові поняття та методи цифрової стеганографії з використанням технології прямого розширення спектра. Нижче описано процес приховування інформаційних повідомлень та їх відновлення на приймальній стороні.

2.1 Приховування і відновлення інформаційних повідомлень

Позначимо інформаційне повідомлення як послідовність $m_0, m_1, ..., m_{k-1}$ з окремих бітів, записаних в полярному вигляді:

$$\forall i \in \{0,1,...,k-1\} : m_i \in \{-1,1\}.$$

Для реалізації технології прямого розширення спектра використовуються дискретні сигнали:

$$\Phi_i \in \Phi = \left\{\Phi_0, \Phi_1, ..., \Phi_{M-1}\right\},\ k \le M,$$

причому кожен сигнал являє собою псевдовипадкову послідовність:

$$\forall i \in \{0,1,...,M-1\} : \Phi_i = \left(\varphi_{i_0}, \varphi_{i_1}, ..., \varphi_{i_{n-1}}\right),$$
$$\forall j \in \{0,1,...,n-1\} : \varphi_{i_j} \in \{-1,1\}.$$

База дискретних сигналів B задає кратність розширення спектра:

$$B = TF,$$

де T - тривалість одного елементарного сигналу φ_{i_j}, F - смуга частот сигналу Φ_i.

Для послідовностей з безлічі Φ маємо:

$$F = n\frac{1}{T},$$

Звідки

$$B = n >> 1,$$

тобто використання $\Phi_i \in \Phi$ дозволяє в n раз розширити спектр частот переданих сигналів.

Передбачається, що різні сигнали з безлічі Φ є слабко корельовані, тобто коефіцієнт їх взаємної кореляції приблизно дорівнює нулю:

$$\forall i \ne j : \rho\left(\Phi_i, \Phi_j\right) = \sum_{u=0}^{n-1} \varphi_{i_u} \varphi_{j_u} \approx 0.$$

Стегано-зображення S формується за допомогою додавання до вихідного зображення C посиленого модульованого сигналу E (1):

$$S = C + G \cdot E, \quad (1)$$

де:

$$E = \sum_{i=0}^{k-1} m_i \Phi_i;$$

$G > 0$ - коефіцієнт посилення, який задає «потужність» модульованого сигналу E.

Відновлення інформаційного повідомлення на приймальній стороні здійснюється за допомогою кореляційного прийому. При цьому передбачається, що кожен сигнал з безлічі Φ, є не корельований з вихідним зображенням (2):

$$\forall i : \rho(\Phi_i, C) \approx 0. \quad (2)$$

Тоді значення коефіцієнта кореляції визначається як:

$$\rho(\Phi_i, S) = \rho(\Phi_i, C + G \cdot E) = \rho(\Phi_i, C) + G \cdot \rho(\Phi_i, E) \approx G \cdot \sum_{j=0}^{k-1} m_j \sum_{u=0}^{n} \varphi_{i_u} \varphi_{j_u}.$$

Для всіх $j \neq i$ остання сума:

$$\sum_{u=0}^{n} \varphi_{i_u} \varphi_{j_u} \approx 0,$$

отже, маємо: $\rho(\Phi_i, S) \approx G \cdot m_i \cdot n$, тобто знак $\rho(\Phi_i, S)$ збігається зі значенням m_i (3):

$$m_i = sign\left(\rho(S, \Phi_i)\right) = \begin{cases} -1, \ \rho(S, \Phi_i) < 0; \\ +1, \ \rho(S, \Phi_i) > 0. \end{cases} \quad (3)$$

У роботах [12-15] проведено експериментальні дослідження, в яких показано, що відновлене за формулою (3) повідомлення містить багато помилок. Дійсно, як видно із табл. 2 [14], інтенсивність бітових помилок знаходиться в діапазоні від 10% до 30%. При цьому нижче 10% помилок не вдалося домогтися навіть використовуючи в (1) дуже високий коефіцієнт посилення G. На нашу думку, основною причиною такого високого рівня помилок є невиконання, в більшості випадків, базового припущення (2). Справді, таке припущення може виконуватися в тому випадку, якщо C є реалізацією природного шуму в КЗ. Однак в даному прикладі під C розуміється *реалістичне зображення* в *цифровому вигляді*. Окремі пікселі цього зображення досить сильно корелюють між собою, і це може призвести до ситуації, коли модуль коефіцієнта кореляції буде значно більше нуля:

$$\left|\rho(\Phi_i, C)\right| >> 0.$$

Якщо

$$\left|\rho(\Phi_i, C)\right| > G \cdot n \quad (4)$$

і одночасно

$$sign\left(\rho(\Phi_i, C)\right) \neq m_i,$$

тоді гарантовано відбудеться помилка в цьому інформаційному біті m_i.

У роботах [12-15] для зменшення помилок у відновлених за правилом (3) інформаційних бітах пропонувалося використовувати складні методи корекції помилок, які засновані на внесенні додаткової надмірності. Це знижує швидкість передачі даних, крім того, підвищує складність обробки на приймальній стороні (*або при зчитуванні з носія даних*).

Авторами даної роботи пропонується інший підхід, коли правило формування дискретних сигналів (*послідовностей з безлічі Ф*) враховує статистичні властивості контейнера C. Іншими словами пропонується використання принципу адаптивної генерації, оскільки кожна ПВП з безлічі Φ формується, адаптуючись виключно під локальну статистику даних контейнера C.

2.2 Адаптивна генерація псевдовипадкових послідовностей

Для реалізації адаптивної генерації послідовностей буде введено обмеження на модуль коефіцієнта кореляції контейнера і формованого сигналу:

$$\forall i : \left|\rho(\Phi_i, C)\right| \leq \rho_{\max}. \quad (5)$$

Значення $\rho_{\max}$ визначає максимально допустиму схожість контейнера C на формований сигнал Φ_i (або на його інверсію $-\Phi_i$). Однак на практиці величина $\rho_{\max}$ не може бути занадто малою, тому що час пошуку потрібних псевдовипадкових послідовностей Φ_i може бути дуже великим. Дійсно, кожен сигнал Φ_i з безлічі Φ формується псевдовипадковим чином (використовуючи для цього генератор псевдовипадкових чисел). При чому використовуються не всі формовані послідовності Φ_i, а тільки ті з них, які задовольняють обмеженню (5). Фактично, відбраковуються ті сигнали, для яких $\left|\rho\left(\Phi_i, C\right)\right| > \rho_{\max}$, і при малих значеннях $\rho_{\max}$ частка відбракованих Φ_i різко зростає.

Слід зазначити, що в разі, коли $\rho_{\max} < G \cdot n$ і одночасно $\forall i \neq j : \rho\left(\Phi_i, \Phi_j\right) = 0,$ то буде забезпечено безпомилкове відновлення потайного інформаційного повідомлення.

Дійсно, в цьому випадку всі сигнали з безлічі Φ взаємно ортогональні, тобто виключається виникнення додаткових взаємних перешкод. Умова (4) не може бути виконана і помилки у відновлених за правилом (3) бітах неможливі (*звичайно, ці міркування справедливі тільки за умови відсутності можливих викривлень стегано-зображення* S).

Процес приховування і відновлення інформаційних повідомлень реалізуються так само, як і у відомих способах, тобто з використанням співвідношення (1), (3). Разом з тим тепер використовувані послідовності з безлічі Φ будуть дійсно некорельовані із зображенням C, тобто припущення (2) буде виконуватися (*зазвичай, для малих* $\rho_{\max}$). Нижче показано, що адаптивна генерація сигналів з безлічі Φ дійсно дозволяє істотно знизити інтенсивність помилок у відновленому повідомленні.

3 Експериментальні дослідження

Для підтвердження вірогідності теоретичної частини були проведені експериментальні дослідження. З використанням системи комп'ютерної математики *Mathcad®* (*від фірми MathSoft*) були реалізовані алгоритми вбудовування та вилучення інформаційних повідомлень в контейнер-зображення з використанням виразів (1) і (2).

Для дослідження процесу приховування повідомлень було обрано напівтонове зображення розміром 256×169 елементів з 8-ми бітовим кодуванням кожного з них (Рис. 1). Для приховування *кожного* інформаційного біту використовувався дискретний сигнал - ПВП довжини $n = 256$. Використовуючи правило (1) було послідовно приховано в кожному з 169 рядків контейнера по $k = 1, 2, ..., 256$ інформаційних бітів. Таким чином, в якості C використовувався один з рядків контейнера і цей експеримент повторювався 169 разів. На наведених нижче графіках вказуються усереднені значення інтенсивності помилок.

Так, на рис. 1 наведено зображення, де:

a) вихідне зображення;

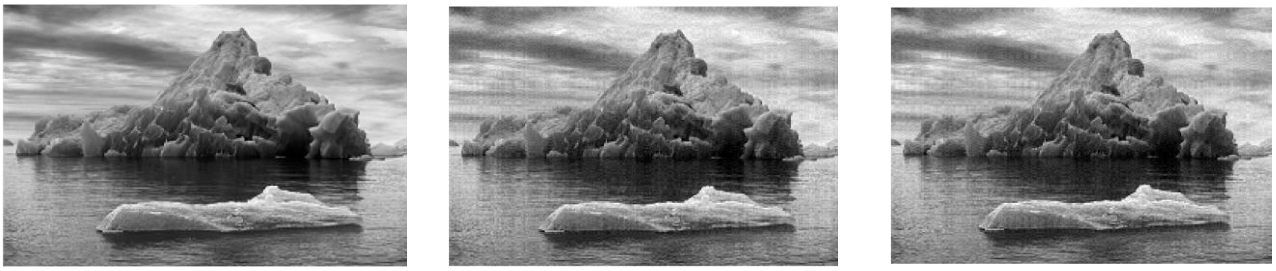
b) зображення після приховування $k = 4$ інформаційних бітів в кожен з рядків контейнера з $G = 4$ *(при цьому використовувалися випадково згенеровані дискретні сигнали)*;

c) зображення після приховування $k = 4$ інформаційних бітів в кожен з рядків контейнера з $G = 4$ *(при цьому використовувалися адаптивно згенеровані дискретні сигнали)*.

Як видно з наведених зображень випадки (b) та (c) *візуально не відрізняються*, тобто адаптивна генерація дискретних сигналів не призводить до підвищення видимих викривлень контейнерів, що використовуються для стегановставки.

В якості дискретних сигналів з множини Φ, використовувалися ПВП, що були зформовані генераторами випадкових чисел *Mathcad®*:

- в разі (b) використовувалися послідовності з рівномірно розподіленими на безлічі {–1,1} послідовностями;
- у разі (c), додатково використовувалось відбраковування дискретних сигналів за правилом (5).

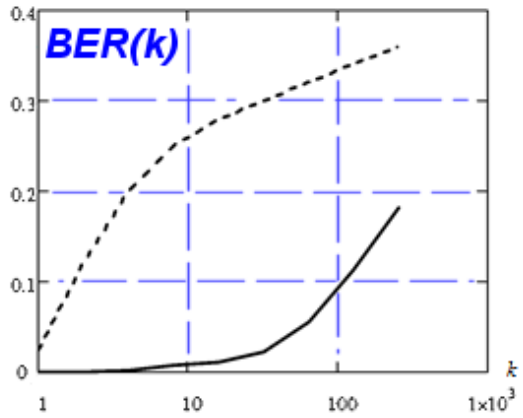


a) *b)* *c)*

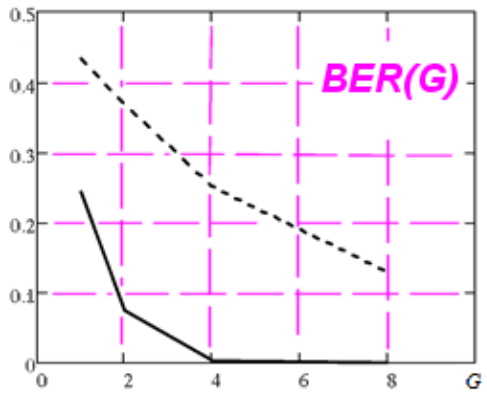
Рис. 1 – Приклади контейнерів-зображень
(помітність спотворень зображення-контейнера)

Найбільш цікавими, на нашу думку, представляються результати досліджень інтенсивності бітових помилок в відновлених повідомленнях. Так, на рис. 2-3 наведені графічні залежності BER для різних умов. Зокрема, на цих рисунках наведені отримані емпіричні залежності BER при відновленні повідомлень за правилом (3), тобто:

- без адаптивної генерації дискретних сигналів (*пунктирна лінія*);
- з використанням адаптивної генерації (*безперервна лінія*).



BER (k)



BER (G)

Рис. 2-3 – BER (k) та BER (G)

При побудові залежностей на рис. 2 використовувалися значення $G = 4$, а k змінювалося в діапазоні від 1 до 255. Як слідує з рис. 2, використання адаптивної генерації, дійсно, дозволяє істотно знизити інтенсивність бітових помилок. Так, навіть при приховуванні 100 і більше інформаційних біт при $G = 4$ вдається досягти низької інтенсивності помилок (*10% і менше*). В контексті цього, нагадаємо, що в роботі [14] було вказано, що таких низьких значень BER не вдавалося досягти навіть при дуже високих значеннях G. Наприклад, при $G = 100$ отримана інтенсивність помилок більше 11% (табл. 2 [14]).

Для залежностей, що відображені на рис. 3, використовувалися значення $k = 4$, а G змінювалося в діапазоні від 1 до 8. При цьому, для розглянутих випадків підвищення коефіцієн-

та посилення дозволяє знизити BER. Однак збільшення G призводить до викривлення зображення-контейнера (див. рис. 1) і т.ч. при $G > 8$ не має практичної доцільності.

Використання адаптивної генерації дискретних сигналів дозволяє істотно знизити BER. Наприклад, при $G > 4$ практично досягається безпомилкове відновлення інформаційних повідомлень. Дійсно, в експериментах були використано $\rho_{\max} = 1000$, що для прийнятих вихідних даних ($G = 4$, $n = 256$) приводить до співвідношення:

$$\rho_{\max} = 1000 < G \cdot n = 1024.$$

Помилки, проте, іноді виникають, тому що застосовані дискретні сигнали не ортогональні (*вони квазіортогональні*):

$$\forall i \neq j : \rho\left(\Phi_i, \Phi_j\right) \approx 0,$$

але інтенсивність помилок істотно знижена (*див. Рис. 2-3*).

При подальшому збільшенні коефіцієнта посилення (тобто при $G > 4$), помилки практично виключені (*див. Рис. 3*).

4 Висновок

В даній роботі було досліджено технологію прямого розширення спектра та її застосування в інтересах стеганографії. Зокрема, розглянуті способи приховування інформаційних повідомлень в зображенні-контейнері, з використанням довгих ПВП (*складних дискретних сигналів з базою* $B = n >> 1$). Основне припущення для побудови таких стеганосистем полягає у відсутності кореляції зображень і використовуваних дискретних сигналів.

Справді, традиційно зображення інтерпретується, як природний шум в КЗ, та для такої інтерпретації, очевидною виглядає статистична незалежність дискретних сигналів і контейнерів. Однак, висока інтенсивність помилок у відновлених повідомленнях спростовує це припущення і наше моделювання це наочно підтверджує.

Пропонується новий підхід, що полягає в адаптивному формуванні дискретних сигналів. В цьому разі, якщо правило формування ПВП буде враховувати статистичні властивості контейнеру, то тоді можна забезпечити виконання базового припущення *про відсутність кореляції зображень і дискретних сигналів*. В межах роботи стверджується, що таку генерацію можна реалізувати, наприклад, найпростішим відбракуванням послідовностей. Для цього потрібно лише ввести обмеження на допустиму корельованість сигналів і зображень, та використовувати, в подальшому, тільки відповідні послідовності.

Проведені експериментальні дослідження підтвердили відповідні теоретичні твердження. Вдалося істотно знизити інтенсивність помилок у відновлених повідомленнях. При цьому, викривлення контейнера залишилися на колишньому рівні.

Важливо зазначити, що використання адаптивної генерації дозволяє реалізувати і безпомилкове відновлення повідомлень. Для цього необхідно вибрати досить суворі обмеження, як на корельованість сигналів і контейнерів, так і на взаємну подобу сигналів один з одним.

Дані експерименти підтверджують практично повну відсутність помилок, що наочно підтверджує достовірність наведених суджень.

Перспективним напрямком подальших досліджень слід розглядати використання дискретних сигналів з особливими кореляційними властивостями, наприклад таких як в [22-26].

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] 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.
[8] V. P. Ipatov, “Spread Spectrum and CDMA,” Mar. 2005. doi:10.1002/0470091800.
[9] “Introduction to CDMA Wireless Communications,” 2007. doi:10.1016/b978-0-7506-5252-0.x5001-7.
[10] “The Generalized CDMA,” CDMA: Access and Switching, pp. 1–28. doi:10.1002/0470841699.
[11] 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.
[12] L. M. Marvel, C. G. Boncelet, R. Jr., and Charles T., “Methodology of Spread-Spectrum Image Steganography,” Jun. 1998. doi:10.21236/ada349102.
[13] 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.
[14] F. S. Brundick and L. M. Marvel, “Implementation of Spread Spectrum Image Steganography,” Mar. 2001. doi:10.21236/ada392155.
[15] 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
[16] 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.
[17] 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.
[18] 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.
[19] 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.
[20] 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.
[21] 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.
[22] 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
[23] 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
[24] 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
[25] 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
[26] 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: Vyacheslav Kalashnikov, Dr. of Sciences (Physics and Mathematics), Full Prof., Department of Systems and Industrial Engineering, Campus Monterrey, Monterrey, Mexico.
E-mail: kalash@itesm.mx

Received on January 2020.

Authors:
Eugene Demenko, Computer Science Student, V. N. Karazin Kharkiv National University, Kharkiv, Ukraine,
E-mail: demenjay@gmail.com

Alexander Onikiychuk, Computer Science Student, V. N. Karazin Kharkiv National University, Kharkiv, Ukraine.
E-mail: onik4524a@gmail.com

Anna Arischenko, Computer Science Student, V. N. Karazin Kharkiv National University, Kharkiv, Ukraine, Ukraine.
E-mail: annaarischenko@gmail.com

Ludmila Gorbachova, Computer Science Student, V. N. Karazin Kharkiv National University, Kharkiv, Ukraine, Ukraine.
E-mail: lusyag23@gmail.com

Oleksii Smirnov, Central Ukrainian National Technical University, Cybersecurity & Software Academic Department, Kropivnitskiy, Ukraine. E-mail: dr.smirnovoa@gmail.com

Adaptive Pseudo-Random Sequence Generation for Spread Spectrum Image Steganography.

Abstract. In this article we consider the ways of data hiding in digital images with the use of pseudorandom sequences and the spread spectrum technique. We propose a new way of the generation of sequences, which considers statistical properties of cover-images. This makes it possible to achieve a low correlation, which provides reliable and safe data hiding in digital images. The results of experimental researches show, that the bit error rate in restored messages is significantly reduced. At the same time, the distortions of cover-images remain the same.

Keywords: Steganography, Data hiding, Digital images, Pseudorandom sequences, Spread spectrum image steganography.

Рецензент: Вячеслав Калашников, д.ф.-м.н., проф., Технологический университет Монтеррея, Монтеррей, Мексика.
E-mail: kuznetsov@karazin.ua

Поступила: Январь 2020.

Авторы:

Евгений Деменко, студент факультета компьютерных наук, ХНУ имени В. Н. Каразина, Харьков, Украина.
E-mail: demenjay@gmail.com

Анна Арищенко, студентка факультета компьютерных наук, ХНУ имени В. Н. Каразина, Харьков, Украина.
E-mail: annaarischenko@gmail.com

Александр Оникийчук, студент факультета компьютерных наук, ХНУ имени В. Н. Каразина, Харьков, Украина.
E-mail: onik4524a@gmail.com

Людмила Горбачова, студентка факультета компьютерных наук, ХНУ имени В. Н. Каразина, Харьков, Украина.
E-mail: lusyag23@gmail.com

Алексей Смирнов, кафедра кибербезопасности и программного обеспечения, Центральный украинский национальный технический университет, Кропивницкий, Украина.
E-mail: dr.smirnovoa@gmail.com

Формирование псевдослучайных последовательностей для сокрытия данных в изображениях.

Аннотация. В статье рассматриваются способы сокрытия данных в цифровых изображениях, с использованием псевдослучайных последовательностей и технологии прямого расширения спектра. Предлагается новый способ формирования последовательностей, который учитывает статистические свойства изображений-контейнеров. Это позволяет добиться низкой корреляции, обеспечивает надежное и безопасное сокрытие информации в цифровых изображениях. Результаты экспериментальных исследований свидетельствуют, что интенсивность битовых ошибок в восстановленных сообщениях, существенно снижена. При этом искажения контейнеров изображений, остаются на прежнем уровне.

Ключевые слова: стеганография; сокрытие данных; цифровые изображения; псевдослучайная последовательность; технология прямого расширения спектра.