Поступила (received) 20.07.2017

Бібліографічні описи / Библиографические описания / Bibliographic descriptions

3D програмно-конфігуровані комутаційні структури на елементах Березовського/ Березовський С. О. // Вісник НТУ «ХПІ». Серія: Механіко-технологічні системи та комплекси. – Харків : НТУ «ХПІ», 2017. – No 20(1242). – С.65–72. – Бібліогр.: 10 назв. – ISSN 2079-5459.

3D программно-конфигурируемые коммутационные структуры на элементах березовского/ Березовский С. А. // Вісник НТУ «ХПІ». Серія: Механіко-технологічні системи та комплекси. – Харків : НТУ «ХПІ», 2017. – No 20(1242). – С.65–72. – Бібліогр.: 10 назв. – ISSN 2079-5459.

3D Program-configurable commutative structures using the elements by Berezovsky/ Berezovsky S. //Bulletin of NTU "KhPI". Series: Mechanical-technological systems and complexes. – Kharkiv: NTU "KhPI", 2017. – № 20 (1242).– P.65–72. – Bibliogr.:10. – ISSN 2079-545

Відомості про авторів / Сведения об авторах / About the Authors

Березовський Станіслав Олександрович – доцент, Одеський національний політехнічний університет, Кафедра Радіотехнічних пристроїв, пр. Т. Г. Шевченко, 1, м. Одеса, Україна, 65044; e-mail: bsa-1@i.ua.

Березовский Станислав Александрович – доцент, Одесский национальный политехнический университет, Кафедра радиотехнических устройств, пр. Т. Г. Шевченко, 1, м. Одеса, Украина, 65044; e-mail: bsa-1@i.ua.

Berezovsky Stanislav – Associate Professor, Odessa National Polytechnic University, Department of Radioengineering Devices, Taras Shevchenko ave., 1, Odesa, Ukraine, 65044; e-mail: bsa-1@i.ua.

УДК 004.056.53

А. Д. СОРОКУН

ДОСЛІДЖЕННЯ МОЖЛИВОСТІ ТА ПЕРСПЕКТИВ ВИКОРИСТАННЯ КАНАЛУ ПЕРЕДАЧІ З МОЖЛИВІСТЮ КОРЕКЦІЇ ПОМИЛОК В ОБЛАСТІ СТЕГАНОГРАФІЇ

Розглядається такий спосіб організації захищеного спілкування двох суб'єктів від атак та ненавмисних змін, як стеганографія. Пропонується використовувати коди з можливістю виправлення помилок, описано механіку й принципи роботи з ними. В експериментальній частині тестується стеганографічна ємність кодів Ріда-Соломона і можливість включення додаткових біт інформації до стеганоповідомлення. Результатом дослідження є обґрунтування перспективи подальших досліджень застосування коригуючих кодів в області стеганографії.

Ключові слова: стеганографія, коригуючі коди, коди Ріда-Соломона, шифрування, мережі зв'язку.

Рассматривается такой способ организации защищенного общения двух субъектов от атак и непреднамеренных изменений, как стеганография. Предлагается использовать коды с возможностью исправления ошибок, описана механика и принципы работы с ними. В экспериментальной части тестируется стеганографическая емкость кодов Рида-Соломона и возможность включения дополнительных бит информации в стеганосообщение. Результатом исследования является обоснование перспективы дальнейших исследований применения корректирующих кодов в области стеганографии.

Ключевые слова: стеганография, корректирующие коды, коды Рида-Соломона шифрования, сети связи.

The present disclosure is directed to several problems relating to the goal of steganography: to hide messages in such a way that no one other than the sender and the intended recipient knows about the existence of this message. It is proposed to use codes with the possibility of correction of errors, also described the mechanics and principles of working with them. In the experimental part, the steganographic capacity of the Reed-Solomon codes is tested. Research field include the possibility of adding additional bits of information to the secret message. The result of the study is to justify the prospect of further research on the use of corrective codes in the area of steganography.

Keywords: steganography, corrective codes, Reed-Solomon codes, Encryption, communication network.

Вступ. У 21 столітті майже всі компанії, державні установи та окремі користувачі спілкуються за допомогою комп'ютерних систем та передових технологій, таких як Інтернет. Сьогодні традиційні паперові носії замінюють своїми цифровими версіями, що дозволяє суттєво зменшити потреби у великих сховищах, а також робить інформацію легкодоступною для більшої кількості користувачів. Майже всі комерційні та приватні організації переходять до "безпаперового" офісу, коли для створення цифрового вмісту все частіше використовуються спільні офісні пристрої, такі як цифрові копіювальні апарати, факсимільні апарати, сканери, цифрові камери та відеокамери. Переваги використання цифрової форми полягає в тому, що її можна легко створювати та зберігати.

Постановка проблеми. Розширення глобальної мережі зв'язку, таких як Інтернет, та посилення залежності від оцифрованої інформації в суспільстві робить інформацію більш вразливою до негативного впливу , і викликає серйозні проблеми щодо безпеки даних та приховування інформації. Забезпечення безпечного спілкування двох суб'єктів, захищене від

атак та ненавмисних змін, є завданням підвищеного рівня складності. Коли спілкування відбувається між двома суб'єктами, які знаходяться в одній і тій самій мережі, проблема одночасної передачі та отримання секретного зображення, без ризику для конфіденційності секретної інформації, є дуже важливою.

Безпека прихованих даних (секретне повідомлення) під час спілкування може реалізуватися двома способами:

використанням техніки секретної комунікації

посиленням стратегії маршрутизації мережі, що використовується під час спілкування

Наука про секретне спілкування у сучасній цифровій епосі вимагає техніки для надійного передавання даних з одного місця в інше. Приклади таких методів включають стеганографію, криптологію, шифрування, цифрові водяні знаки та відбитки пальців. Дана стаття буде стосуватись проблем стеганографії.

Стеганографія – це наука про прихований зв'язок. Мета стеганографії полягає в тому, щоб приховати повідомлення таким чином, щоб ніхто, крім відправника та передбачуваного одержувача, не знав про існування цього повідомлення. Прихована інформація не привертає уваги і не піддається атакам. Цей підхід відрізняється від криптографії, метою якої є зробити інформацію такою, яку неможливо прочитати.

Ціль та задачі дослідження. Метою дослідження є можливість використання в області стеганографії типу каналу передачі з можливістю корекції помилок.

Задачею дослідження я ставлю виділення методу, який можна використовувати для подальших досліджень як основу.

Шифрування даних. Теорія шифрування – це «вивчення методів ефективної і точної передачі інформації з одного місця в інше». З математичної точки зору, шифрування – це ін'єкція, яка присвоює кожному символу з набору A символ з набору Y. Таким чином, створюється кодове слово C_i. Код являє собою набір всіх кодових слів. Кодові слова C_i представлені у вигляді кратної послідовності, де кожному з об'єктів m відповідає стан Z. Довжина коду L – це кількість кодових слів C_i. Ця довжина для бінарних кодів визначається співвідношенням $1 \le L \le 2^m$.

Основною ідеєю шифрування є те, що всі кодові слова повинні бути такими, що диференціюються один з одним. З цією метою в теорію шифрування було введено поняття відстані між кодовими словами. Доти доки два кодових слова зпівставлюються один з одним, вони повинні мати однакову відстань.

Типи коригуючих кодів. Існує кілька аспектів, за якими коди можуть бути розділені.

I. Шлях додавання розмірностей:

1. Систематичні коди: з інформаційних бітів k одержуються надлишкові біти (r = n – km, де n – довжина кодового слова). Кодове слово складається з інформаційних бітів, за якими слідують надлишкові біти. Інформаційні біти повідомлення відділяються від надлишкових бітів під час передачі. Систематичні коди позначені як коди (n,k).

2. Не систематичні коди: інформаційні біти замінюються послідовностями бітів з більш високою надлишковістю. В процесі передачі не представляється можливим відмежовувати надлишкові біти від інформаційних бітів.

II. Шлях виправлення помилок:

1. Коди виявлення: помилки тільки ідентифікуються і не виправляються відразу. Корекція може бути виконана шляхом запиту на повтор передачі помилкового сегмента.

2. Коригувальні коди: помилки ідентифікуються і виправляються відразу ж, без необхідності зворотного запиту. Обчислювальна складність, а також можливості корекції визначається кодом виправлення помилок і його технічними характеристиками.

Існує дві групи кодів:

1. Кодування джерела (кодування ентропії): це процес стиснення вихідних даних для того, щоб отримати більш високу ефективність передачі.

2. Кодування каналу (пряме виправлення помилок): це процес додавання надлишкових бітів до повідомлення, щоб забезпечити стійкість до шуму зв'язку.

Алгебраїчна теорія коду розрізняє два класи кодів корекції помилок:

1. Коди лінійних блоків

2. Конволюційні коди

Коди лінійних блоків обробляють повідомлення блок за блоком. Кожен блок не залежить від інших блоків, тобто коди блоків не мають пам'яті. Властивість лінійності означає, що сума, а також скалярний добуток будь-яких двох кодових слів дає ще одне кодове слово

Конволюційні коди, на відміну від кодів лінійних блоків, залежать не тільки від поточної вхідної інформації, але і від попередніх входів і виходів блоку за блоком або біту за бітом. Для цього конвоюційний кодер має пам'ять і, таким чином, являє собою завершений механізм. Статус датчика визначається вмістом його пам'яті. Процес дешифрування виконується за допомогою алгоритму Viterbi.

Основна мета шифрування полягає в запобіганні виникненню помилок в переданому повідомленні. Канал передачі забезпечує передачу повідомлення між відправником і отримувачем. На рис. 2 показано місце, де помилки можуть виникати через перекручування і шуми.

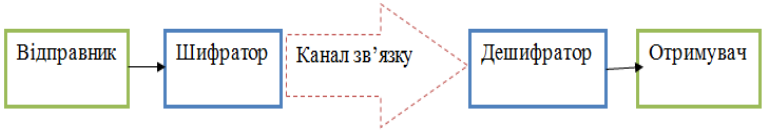

Рис.1 – Виникнення помилок

При шифруванні розпізнають такі два класи помилок:

1. Помилки поодиноких бітів (незалежні помилки): вони викликані шумом, який впливає тільки на один елемент сигналу. Різні статичні характеристики визначаються для того, щоб описати їх властивості. У послідовності бітів тільки одна помилка. Якщо відбуваються множинні помилки, це означає, що в послідовності бітів існує більше незалежних помилок.

2. Пакет помилок: це послідовності переданих сигнальних елементів, в яких частота помилкових елементів вища, ніж частота правильно переданих елементів.

Поля Галуа і коди Ріда-Соломона. В теорії шифрування використовується арифметика скінченних полів. Скінченні поля були досліджені французьким математиком Галуа, і тому вони називаються полями Галуа (GF). Скінченні поля є структурою алгебри, в якій існують основні математичні операції, такі як додавання, віднімання, множення і ділення між його елементами. Для всіх елементів GF є вірним те, що результат будь-якої операції є елементом поля. Скінченні поля складаються зі скінченного числа елементів.

Оптимальними для використання в стегоканалі є коди Ріда-Соломона, що являють собою блокові коди виправлення помилок. Введення складається з блоків даних, до якої кодер додає надлишкові (парні) дані. Надлишкові дані використовуються для відновлення пошкоджених даних, викликаних шумом в процесі передачі даних. Кількість і тип помилок, які можуть бути виправлені, залежить від характеристик коду Ріда-Соломона.

Для інформаційних символів кодер додає символи парності, вихідним сигналом якого є кодове слово довжиною n символів. Таким чином, число символів парності дорівнює (n–k), кожний довжиною m біт. Не двійковість означає, що символ складається з більш ніж одного біта. Декодер Ріда-Соломона дозволяє коригувати до t символів в кодовому слові, де 2t = n–k. Число парних символів прямо пропорційно ефективності і кількості символів, який є код може виправити.

Обчислювальна складність шифрування і дешифрування кодів Ріда-Соломона, прямо пропорційна кількості символів парності в кодовому слові. Чим більше символів парності прикріплено до інформаційних символів, тим більше помилок код може виправити, але це вимагає більше обчислювальної здатності.

Код Ріда-Соломона може бути концептуально вкорочений так, що використовуватимуться не всі інформаційні символи. Надлишкові символи обчислюються з усіх (також нульових) інформаційних символів, проте передається тільки використана частина інформаційних символів. Декодер додає назад нульові інформаційні символи і дешифрує повідомлення.

Результати дослідження. Було виконано експериментальне дослід-ження, з метою визначення оптимальної організації експерименту. В якості кода Ріда-Соломона, був використаний код RS (31,23) з 5-бітових символів, інформація, що складається з 23 символів, з можли-вістю корекції до 4-х символів помилок. В кожне кодове слово вбудовано 2 стеганографічні біти (t/2). Характеристика цього коду являє собою компроміс між продуктивністю і стеганографічною обчислю-вальною ефективністю. На даний час немає загально-прийнятих тестів або стандартів для оцінки стегано-графічних алгоритмів, проте, загальні принципи та основні положення слід враховувати при розробці стеганографічного методу. Тому, на основі експери-ментальних досліджень основного положення та інших подібних досліджень, я обрав три наступні показники для вимірювання при перевірці:

1. Однорідність розподілу помилок

2. Співвідношення успішного дешифрування інформації

3. Співвідношення успішного дешифрування стеганографічної інформації

Співвідношення успішного дешифрування інформації визначає, як стеганографічна модифікація впливає на можливості корекції помилок кодів Ріда-Соломона. Часті збої в успішному дешифруванні переданої інформації вказують на недостатню характеристику коду, обрану для конкретного застосування. Це буде означати, наявність стеганографічних даних і, таким чином, виявляється приховане повідомлення.

Співвідношення успішного дешифрування стеганографічної інформації визначає успішність стеганографічного дешифрування даних.

Рівномірність картини розподілу помилок залишається подібним шляхом повторення тестів, в різний час, як це показано на рис. 2. Проте стандартне відхилення збільшується за рахунок збільшення числа тестових повторень, що природно, і наведено в табл. 1.

Порівнюючи співвідношення успішного дешифрування інформації контейнеру і стеганографічної інформації, я виявив, що відмінності незначні. Співвідношення успішного дешифрування інформації склала 100 % для кожного числа повторень і співвідношення успішного дешифрування стеганографічної інформації була в середньому 98,63 %, як описано в табл. 2.

Таблиця 1 – Пілотне дослідження – стандартне відхилення частоти місця помилки

Кількість тестів	Стандартне відхилення частоти місця помилки	Тривалість тесту (хв.)
1 000	3.81	7
5 000	7.38	36
10 000	11.32	64
20 000	16.16	141

Таблиця 2 – Пілотне дослідження – порівняння успішних дешифрувань

Кількість тестів	Кількість успішних дешифрувань інформації	Кількість успішних дешифрувань стеганографічної інформації
1 000	1 000 (100 %)	986 (98.60 %)
5 000	5 000 (100 %)	4935 (98.70 %)
10 000	10 000 (100 %)	9868 (98.68 %)
20 000	20 000 (100 %)	19717 (98.59 %)

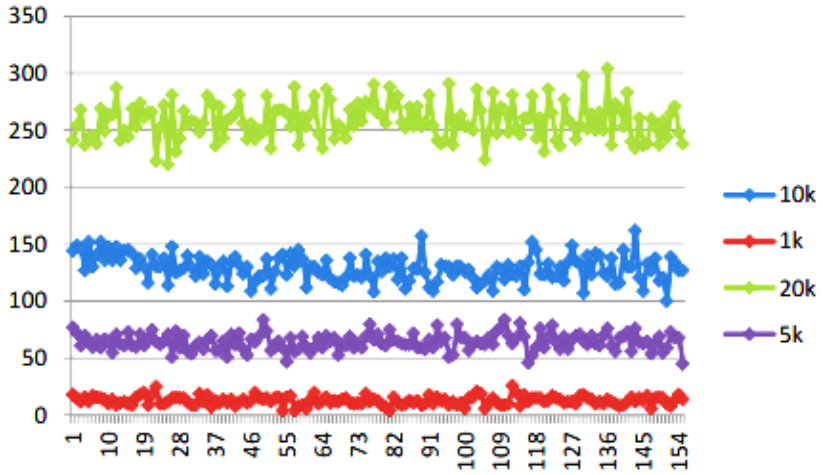

Рис. 2 – Відношення частоти до помилок

Висновки. Обидва експерименти підтвердили гіпотезу, висловлену на початку: стеганографічні дані можуть бути приховані в каналі Ріда-Соломона, який задовольняє первинні атрибути алгоритму стеганографії. В ході випробувань ємності коду Ріда-Соломона з виправлення помилок жодного разу не була перевищена. Таким чином, виявлення стеганографії значно знижується.

Список літератури:

1. *Кохановић, Г. Ф.* Комп'ютерна стеганографія. Теорія і практика [Текст] / *Г. Ф. Кохановић, А. Ю. Пузиренко*. – Київ: «МК-Пресс», 2006. – 288 с.
2. *Ватолин, Д.* Методи стиснення даних. Пристрій архіваторів, стиснення зображень і відео [Текст] / *Д. Ватолин, А. Ратушняк, М. Смирнов, В. Юкін*. – М.: «ДІАЛОГ-МІФІ», 2003. – 384 с.
3. *Шеннон, К.* Работы по теории информации и кибернетике [Текст] / *К. Шеннон*. – М.: Иностранная литература, 1963. – 832 с.
4. *Рудой, В. М.* Системы передачи информации [Текст] / *В. М. Рудой*. – М.: МГОУ, 2004. – 171 с.
5. *Бройдо, В.* Вычислительные системы, сети и телекоммуникации [Текст] / *В. Бройдо*. – СПб.: Питер, 2002. – 688 с.
6. *Yevseiev, S.* Developing of multi-factor authentication method based on niederreiter-mceliece modified crypto-code system [Text] / *S. Yevseiev, K. Hryhorii, Y. Liekariev* // Eastern-European Journal of Enterprise Technologies. – 2016. – No. 6/4 (84). – P. 11–23. doi:10.15587/1729-4061.2016.86175
7. *Horbenko, Iu. Y.* Development of mathematical and software models of the perspective encryption algorithm for implementation verification [Text] / *Iu. Y. Horbenko, R. I. Mordvynov, O. O. Kuznetsov* // Eastern-European Journal of Enterprise Technologies. – 2014. – No. 5/9 (71). – P. 39–45. doi:10.15587/1729-4061.2014.28010
8. *Andrushchenko, D. M.* The method of the internet authorization for the protection of shareware programs [Text] / *D. M. Andrushchenko, H. L. Kozyna* // Eastern-European Journal of Enterprise Technologies. – 2014. – No. 4/2 (70). – P. 23–27. doi:10.15587/1729-4061.2014.26302
9. *Zheleznjak, A. A.*Ensuring the invariance of the pattern recognition system of the marine vessel systems in the process of fishing [Text] / *A. A. Zheleznjak, Ju. F. Katorin, N. P. Smetjuh, V. A. Dorovskoj, S. G. Chernyj* // Eastern-European Journal of Enterprise Technologies. – 2015. – No. 6/2 (78). 47–54. doi: 10.15587/1729-4061.2015.55696
10. *Zhilenkov, A.*Investigation Performance of Marine Equipment with Specialized Information Technology [Text] / *A. Zhilenkov, S. Chernyi* // Procedia Engineering. – 2015. – No. 100. – P. 1247–1252. doi: 10.1016/j.proeng.2015.01.490

Bibliography (transliterated):

1. Kokhanovych, H. F., Puzyrenko, A. Iu. (2006). Kompiuterna stehanohrafiia. Teoriia i praktyka. Kyiv: «MK-Press», 288.
2. Vatolyn, D., Ratushniak, A., Smyrnov, M., Yukin, V., Vatolyn, D. (2003). Metody stysnennia danykh. Prystrii arkhivatoriv, stysnennia zobrazhen i video, Moscow: «DIALOH-MIFI», 384.
3. Shennon, K. (1963). Raboty po teorii informacii i kibernetike. Moscow: Inostrannaja literatura, 832.
4. Rudoj, V. M. (2004). Sistemy peredachi informacii. Moscow: MGOU, 171.
5. Brojdo, V. (2002). Vychislitel'nye sistemy, seti i telekommunikacii. Saint Petersburg: Piter, 688.
6. Yevseiev, S., Hryhorii, K., & Liekariev, Y. (2016). Developing of multi-factor authentication method based on niederreiter-mceliece modified crypto-code system. Eastern-European Journal of Enterprise Technologies, 6(4 (84)), 11–23. doi:10.15587/1729-4061.2016.86175
7. Horbenko, Iu. Y., Mordvynov, R. I., Kuznetsov, O. O. (2014). Development of mathematical and software models of the perspective encryption algorithm for implementation verification. Eastern-European Journal of Enterprise Technologies, 5(9(71)), 39. doi:10.15587/1729-4061.2014.28010
8. Andrushchenko, D. M., Kozyna, H. L. (2014). The method of the internet authorization for the protection of shareware programs. Eastern-European Journal of Enterprise Technologies, 4(2 (70)), 23–27. doi:10.15587/1729-4061.2014.26302
9. Zheleznjak, A. A., Katorin, Ju. F., Smetjuh, N. P., Dorovskoj, V. A., Chernyj, S. G. (2015). Ensuring the invariance of the pattern recognition system of the marine vessel systems in the process of fishing. Eastern-European Journal of Enterprise Technologies, 6(2(78)), 47–54. doi:10.15587/1729-4061.2015.55696
10. Zhilenkov, A., Chernyi, S. (2015). Investigation Performance of Marine Equipment with Specialized Information Technology. Procedia Engineering, 100, 1247–1252. doi:10.1016/j.proeng.2015.01.490

Надійшла (received) 20.07.2017

Бібліографічні описи / Библиографические описания / Bibliographic descriptions

Дослідження можливості та перспектив використання каналу передачі з можливістю корекції помилок в області стеганографії/ Сорокун А. Д. // Вісник НТУ «ХПІ». Серія: Механіко-технологічні системи та комплекси. – Харків : НТУ «ХПІ», 2017. – No 20(1242). – С.72–76. – Бібліогр.: 10 назв. – ISSN 2079-5459.

Исследование возможности и перспектив использования канала передачи с возможностью коррекции ошибок в области стеганографии/ Сорокун А. Д. // Вісник НТУ «ХПІ». Серія: Механіко-технологічні системи та комплекси. – Харків : НТУ «ХПІ», 2017. – No 20(1242). – С.72–76. – Бібліогр.: 10 назв. – ISSN 2079-5459.

Investigation of the possibility and prospects of using the transmission channel with the possibility of correction of errors in the field of steganography/ Sonokun A. //Bulletin of NTU “KhPI”. Series: Mechanical-technological systems and complexes. – Kharkov: NTU “KhPI”, 2017. – № 20 (1242).– P.72–76. – Bibliogr.:10. – ISSN 2079-545

Відомості про авторів / Сведения об авторах / About the Authors

Сорокун Антон Дмитрович – аспірант, Київський національний авіаційний університет, Кафедри комп'ютеризованих систем захисту інформації; пр. Космонавта Комарова, 1, м. Київ, Україна, 02000; anton.sorokun@gmail.com.

Сорокун Антон Дмитриевич – аспирант, Киевский национальный авиационный университет, Кафедры компьютеризированных систем защиты информации; пр. Космонавта Комарова, 1, г. Киев, Украина, 02000; anton.sorokun@gmail.com.

Sonokun Anton – post-graduate student, Kiev National Aviation University, Department of computerized information security systems; ave Cosmonaut Komarova, 1, Kiev, Ukraine, 02000; Anton.sorokun@gmail.com.