Информатика. Экономика. Управление// Informatics. Economics. Management

2024; 3(2) http://oajiem.com/

УДК: 004.056.5
DOI: https://doi.org/10.47813/2782-5280-2024-3-2-0415-0424

EDN: **MPYZSM**

Математическая модель защищенного канала связи для морских исследований методом стеганографии

И. Н. Карцан

ФГБУН ФИЦ «Морской гидрофизический институт РАН», г. Севастополь, Россия

Аннотация. Все больше внимание уделяется способам передачи информации между морскими исследовательскими приборами и пунктами сбора и обработки информации для дальнейшего анализа и выработки концепций развития Мирового океана. Вся передаваемая информация подвержена получению третьими лицами, в связи с этим, стоит одна из задач, защита передаваемой информации. Не исключение составляет и организованный канал передачи информации между морской платформой и берегом на Черноморском гидрофизическом подспутниковом полигоне. Представленная математическая модель на основе метода стеганографии позволяет решить задачу подтверждения подлинности путем внедрения дополнительной информации в исходный сигнал, таким образом, что факт внедрения не будет распознан эмпирически. Одним из первых и наиболее известным методом скрытного внедрения дополнительной информации является метод на основе технологии расширения спектра и множественные его модификации, основанные на внедрении в математическую формулу дополнительных коэффициентов, призванных усовершенствовать метод. Однако, при кодировании дополнительной информации введение в исходный звуковой сигнал коэффициентов оказывает влияние на скрытность и изменяет устойчивость, что может привести к разрушению стегосистемы. Поэтому совершенствование методов стеганографии, с одной стороны, направлено на повышение скрытности, а с другой стороны, на повышение стойкости.

Ключевые слова: защита информации, информационные технологии, алгоритм, акустический сигнал, стеганография.

Благодарности: Работа выполнена в рамках государственного задания по теме № FNNN-2024-0016.

Для цитирования: Карцан, И. Н. (2024). Математическая модель защищенного канала связи для морских исследований методом стеганографии. Информатика. Экономика. Управление - Informatics. Economics. Management, 3(2), 0415–0424. https://doi.org/10.47813/2782-5280-2024-3-2-0415-0424

Mathematical model of secure communication channel for marine research by steganography method

Igor Kartsan

FSBUN FIC "Marine Hydrophysical Institute of the Russian Academy of Sciences", Sevastopol, Russia

Abstract. Increasing attention is being paid to the ways in which information can be transmitted between marine research instruments and data collection and processing facilities, for further analysis and conceptualization of the development of the world's oceans. All transmitted information is susceptible to acquisition by third parties and therefore one of the challenges is to protect the transmitted information. The organized channel of information transmission between the offshore platform and the shore at the Black Sea hydrophysical sub-satellite test site is not an exception. The presented mathematical model of steganography method allows to solve the problem of authentication by introducing additional information into the original signal, so that the fact of introduction will not be recognized empirically. One of the first and most well-known method of covertly introducing additional information, is a method based on the technology of spectrum expansion and its multiple modifications, based on the introduction of additional coefficients in the mathematical formula, designed to improve the method. However, when encoding additional information into the original audio signal, the coefficients, affect the covertness and change the stability, which can lead to the destruction of the stego system. Therefore, the improvement of steganography methods, on the one hand, is aimed at improving the stealth and, on the other hand, at improving the robustness.

Keywords: information protection, information technologies, algorithm, acoustic signal, steganography.

Acknowledgements: The work was performed within the framework of the state assignment under the topic No. FNNN-2024-0016.

For citation: Kartsan, I. N. (2024). Mathematical model of secure communication channel for marine research by steganography method. Informatics. Economics. Management, 3(2), 0415–0424. https://doi.org/10.47813/2782-5280-2024-3-2-0415-0424

ВВЕДЕНИЕ

Широкое распространение и совершенствование вычислительных систем и информационных технологий привело к росту их пропускной способности, все большей интеграции в сферу предоставления услуг, а также формированию новых технологий обработки, передачи и хранения информации. В результате чего возросло количество и сложность новых угроз обеспечению безопасности информации, помимо этого вопрос подтверждения подлинности информации обретает все большую актуальность. Одним из путей решения задач совместного обеспечения конфиденциальности, доступности и целостности информации достигается применением криптографических и

стеганографических методов ее защиты. [1] Однако, применение криптографических методов защиты информации не всегда целесообразно для широкого потребителя в виду сложности механизмов реализации, стеганографические же методы лишены такого недостатка.

В современном цифровом мире стеганография может иметь разные цели, в частности, одно из наиболее востребованных приложений стеганографии — защита авторского права [2, 3] при помощи кодирования дополнительной информации — «водяного знака».

Цифровые стеганографические методы сокрытия информации и сама стеганография как наука начала свое становление из иной технологии сокрытия информации, известной как «криптография» [4].

Функционально методы стеганографии направлены на сокрытие самого факта передачи информации, за счет ее «маскирования» [5]. Идеальный стеганографический метод скрывает большой объем информации, гарантируя, что измененный объект визуально или на слух не будет отличим от исходного объекта.

Цифровая стеганография как наука родилась в последние годы [6], в результате чего в России отсутствует нормативно-правовая база, регламентирующая и однозначно определяющая принципы, классификацию методов, цели использования стеганографии и терминологию, в связи с чем в различных источниках даются различные трактовки одного и того же термина [1]. В 1996 году на конференции «Information Hiding: First Information Workshop» [7, 8] в статье «Information Hiding Terminology» [9] было предложено использовать единую терминологию.

Термин «стеганография» означает способ передачи (или хранения) информации, при котором сохраняется в тайне факт такой передачи (или хранения). При этом под скрытой (стеганографической) передачей информации подразумевают методы передачи дополнительной информации в избыточных структурах данных, представленных в цифровом виде и используемых в качестве контейнера [10-18].

АЛГОРИТМ КОДИРОВАНИЯ

Для определения наиболее стойкого шумоподобного сигнала при передаче по каналам связи в математической модели будут применены следующие характеристики:

- Уменьшение частоты дискретизации сигнала, содержащего цифровой водяной знак до 8 кГц и увеличение обратно до 16 кГц;

- Изменение шага квантования сигнала, содержащего цифровой водяной знак до 8 бит/значение, а затем повышение шага квантования сигнала до 16 бит/значение;
- Применение фильтра нижних частот с частотой среза 4 кГц;
- Применение фильтра нижних частот с частотой среза 8 кГц;
- Масштабирование амплитуды речевого сигнала, содержащего цифровой водяной знак до 0.85 от текущего значения;
- Добавление белого гауссова шума с нулевым средним значением к речевому сигналу, содержащего цифровой водяной знак с соотношением сигнал/шум SNR = 30 dB;
- Добавление белого гауссова шума с нулевым средним значением к речевому сигналу, содержащего цифровой водяной знак с соотношением сигнал/шум SNR = 20 dB;
- Сдвиг во времени речевого сигнала, содержащего цифровой водяной знак на одно декретированное значение;
- Сдвиг во времени речевого сигнала, содержащего цифровой водяной знак на три декретированных значения.

Алгоритм кодирования дополнительной информации (сообщения) условно можно разделить на 2 уровня. На первом уровне (предкодере) производится преобразование алфавита передаваемого сообщения, подготовительная модуляция сгенерированного шумоподобного сигнала, формирование базы, содержащей количество отрезков, в которые будет кодироваться информация.

Первый уровень:

1. Разбиение звукового сигнала ($\vec{x} = [x_1, x_2, .., x_N]$), на отрезки длиной $\vec{c} = 1024$, где N – количество отрезков.
2. Нормирование по амплитуде [-1;1] шумоподобного сигнала:

$$\vec{m}_n = \frac{max(\vec{u}) + min(\vec{u})}{2}, \quad (1)$$

где $max(.)$ – максимальное значение амплитуды $\vec{u}$; $min(.)$ – минимальное значение амплитуды u.

3. Приведение алфавита передаваемого сообщения ($\vec{M} = \{m_1, m_2, .., m_l, .., m_L, \}$, где L – количество элементов) к виду $e \in \{-1; 1\}$, где e – бит информации.
4. Вычисление энергии шумоподобного сигнала (E_u);

$$E_u = \sum_{i=0}^{c} {u_i}^2, \quad (2)$$

где c – длина отрезка; u_i – элемент шумоподобного сигнала.

5. Нормирование энергии шумоподобного сигнала (u_n):

$$\vec{u}_n = \frac{\vec{u}}{\sqrt{E_u}}. \quad (3)$$

6. Вычисление коэффициента фильтрации (α):

$$\vec{\alpha} = \langle \vec{c} \cdot \vec{u}_n \rangle. \quad (4)$$

7. Формирование цифрового водяного знака (w_n):

$$\vec{w}_n = e \cdot |\vec{\alpha}| \cdot \vec{u}_n . \quad (5)$$

На втором уровне (кодере) производится фильтрация и внедрение цифрового водяного знака в каждый отрезок длиной $\vec{c}$ = 1024 звукового сигнала ($\vec{x} = [x_1, x_2, .., x_N]$), где N – количество отрезков:

$$\vec{y} = \vec{c} - \vec{\alpha} \cdot \vec{u}_n + \vec{w}_n . \quad (6)$$

На рисунке 1 представлена модернизированная модель расширения спектра, основанная на ряде математических преобразований шумоподобного сигнала.

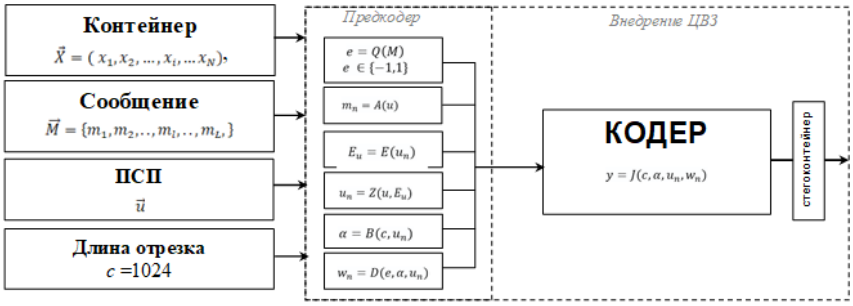

Рисунок 1. Схема преобразований информации, протекающих в кодере.

Figure 1. Scheme of information transformations occurring in the encoder.

ИЗВЛЕЧЕНИЕ ИНФОРМАЦИОННЫХ СИГНАЛОВ

Схема извлечения информации (сообщения) имеет вид, представленный на рисунке 2.

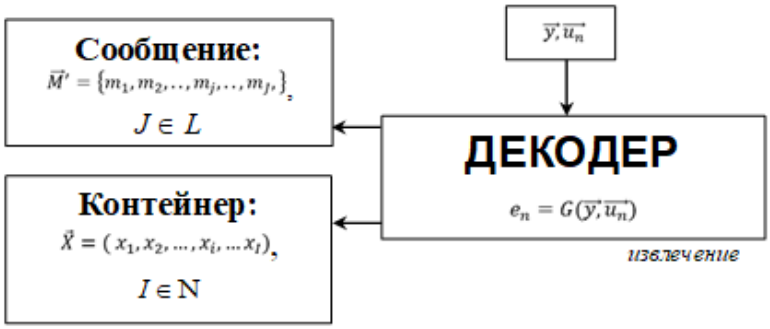

Рисунок 2. Схема преобразований информации, протекающих в декодере.

Figure 2. Scheme of information transformations occurring in the decoder.

Извлечение бита (e_n) информации происходит согласно формуле:

$$e_n = sign(\langle \vec{y}, \vec{u}_n \rangle), \quad (7)$$

где e_n – восстановленный элемент цифрового водяного знака, принимающий значения $e_n \in \{-1; 1\}$; $sign()$ – функция определения знака; $\langle .,. \rangle$ – скалярное произведение векторов, принимающее вид:

$$\langle \vec{y}, \vec{u}_n \rangle = \sum_{i=1}^{I} y_i \cdot \vec{u}_{ni}\,, \quad (8)$$

где y_i – элемент полученного стегаконтейнера $\vec{y}$; $\vec{u}_{ni}$ – элемент полученного нормированного шума $\vec{u}_n$.

ЗАКЛЮЧЕНИЕ

Таким образом, предложена модель расширения спектра, использующая заданный параметры выбранных шумов, для проведения дальнейших экспериментов с целью оценки эффективности.

Одной из проблем, связанной с цифровой стеганографией, является многообразие задач и требований в зависимости от приложения, в результате чего одна и та же задача может быть решена несколькими методами, что затрудняет процесс выделения обособленной области применения. Проанализировав текущее применение и конечное назначение стеганографических алгоритмов можно условно выделить следующие области ее применения:

- защита от копирования;
- скрытие части документа;
- аутентификация;
- скрытая связь.

Помимо вышеописанных областей стеганографические методы могут быть применены в новой области, в будущем они могут помочь решить назревающую беспрецедентную проблему, связанную с прогрессирующими возможностями и широким распространением искусственного интеллекта.

СПИСОК ЛИТЕРАТУРЫ

[1] Абазина Е.С., Ерунов А.А. Цифровая стеганография: состояние и перспективы. Системы управления, связи и безопасности. 2016; 2. URL: https://masters.donntu.ru/2020/fknt/kukhta/library/ar6.pdf (дата обращения: 25.05.2024).

[2] Белкина Т.А. Аналитический обзор применения сетевой стеганографии для решения задач информационной безопасности. Молодой ученый. 2018; 11(197): 36-44.

[3] Иванников А.Д., Кулагин В.П., Тихонов А.Н., Цветков В.Я. Цифровая стеганография: шифрование, защита. Информационные технологии. 2004; 8: 1-32.

[4] Нуриев С.А., Карцан И.Н. Совершенствование цифровых каналов связи. Защита информации. Инсайд. 2023; 5(113): 5-9.

[5] Толстошев А.П., Лунев Е.Г., Мотыжев С.В., Дыкман В.З. Модуль оценивания солености морской воды на основе измерений скорости звука. Морской гидрофизический журнал 2021; 37(1): 132–142. https://doi.org/10.22449/0233-7584-2021-1-132-142

[6] Мордвинова А.Ю., Нуриев С.А. Исследование уязвимостей и угроз безопасности стандарта IEEE 802.11. Современные инновации, системы и технологии. 2023; 3(3): 0117-0131. https://doi.org/10.47813/2782-2818-2023-3-3-0117-0131

[7] Нуриев С.А., Карцан И.Н. Защищенность речевой информации в научных организациях от утечки по техническим каналам. Современные инновации, системы и технологии. 2023; 3(4): 0349-0362. https://doi.org/10.47813/2782-2818-2023-3-4-0349-0362

[8] Нуриев С.А. СУБД в архитектуре ГИС нового поколения. В сборнике: Вопросы контроля хозяйственной деятельности и финансового аудита, национальной безопасности, системного анализа и управления. материалы VII Всероссийской научно-практической конференции. Москва; 2022: 525-529.

[9] Петренко А.С., Петренко С.А., Костюков А.Д., Ожиганова М.И. Модель квантовых угроз безопасности для современных блокчейн-платформ. Защита информации. Инсайд. 2022; 3(105): 10-20.

[10] Петренко А.С., Петренко С.А., Антонова-Дружинина А.О., Ожиганова М.И. Метод параметрического выбора криптопримитивов для квантово-устойчивой блокчейн-платформы. Часть I. Защита информации. Инсайд. 2022; 4(106): 24-33.

[11] Попов А.Ю., Ремез М.В., Жилина Е.В., Ожиганова М.И. Парсинг электронных ресурсов. библиотека selenium или fake user agent? Информатизация в цифровой экономике. 2022; 4(3): 197-210. https://doi.org/10.18334/ide.3.4.115219

[12] Ожиганова М.И., Шейко А.О., Исакова Е.М., Миронова А.О. Методы и средства проведения анализа угроз локальной вычислительной сети предприятия. В сборнике: Цифровая трансформация науки и образования. Сборник научных трудов II Международной научно-практической конференции. 2021: 264-270.

[13] Петренко А.С., Петренко С.А., Ожиганова М.И. Оценка возможностей квантовых алгоритмов криптоанализа. Защита информации. Инсайд. 2021; 6(102): 70-82.

[14] Ожиганова М.И., Куртаметов Э.С. Применение машинного обучения в защите веб-приложений. НБИ технологии. 2020; 2(14): 16-20. https://doi.org/10.15688/NBIT.jvolsu.2020.2.3

[15] Калита А.О., Ожиганова М.И., Тищенко Е.Н. Основы организации адаптивных

систем защиты информации. НБИ технологии. 2019; 1(13): 11-15.

[16] Ожиганова М.И., Калита А.О., Тищенко Е.Н. Построение адаптивных систем защиты информации. НБИ технологии. 2019; 4(13): 12-21.

[17] Аверьянов В.С., Карцан И.Н. Методы оценки защищенности автоматизированных систем на базе квантовых технологий согласно CVSSV2.0/V3.1, Защита информации. Инсайд. 2023; 1(109): 18-23.

[18] Карцан И.Н., Жуков А.О. Механизм защиты промышленной сети, Информационные и телекоммуникационные технологии, 2021; 52: 19-26.

REFERENCES

[1] Abazina E.S., Erunov A.A. Cifrovaya steganografiya: sostoyanie i perspektivy. Sistemy upravleniya, svyazi i bezopasnosti. 2016; 2. (in Russian) URL: https://masters.donntu.ru/2020/fknt/kukhta/library/ar6.pdf (data obrashcheniya: 25.05.2024).

[2] Belkina T.A. Analiticheskij obzor primeneniya setevoj steganografii dlya resheniya zadach informacionnoj bezopasnosti. Molodoj uchenyj. 2018; 11(197): 36-44. (in Russian)

[3] Ivannikov A.D., Kulagin V.P., Tihonov A.N., Cvetkov V.YA. Cifrovaya steganografiya: shifrovanie, zashchita. Informacionnye tekhnologii. 2004; 8: 1-32. (in Russian)

[4] Nuriev S.A., Karcan I.N. Sovershenstvovanie cifrovyh kanalov svyazi. Zashchita informacii. Insajd. 2023; 5(113): 5-9. (in Russian)

[5] Tolstoshev A.P., Lunev E.G., Motyzhev S.V., Dykman V.Z. Modul' ocenivaniya solenosti morskoj vody na osnove izmerenij skorosti zvuka. Morskoj gidrofizicheskij zhurnal 2021; 37(1): 132–142. (in Russian) https://doi.org/10.22449/0233-7584-2021-1-132-142

[6] Mordvinova A.YU., Nuriev S.A. Issledovanie uyazvimostej i ugroz bezopasnosti standarta IEEE 802.11. Sovremennye innovacii, sistemy i tekhnologii. 2023; 3(3): 0117-0131. https://doi.org/10.47813/2782-2818-2023-3-3-0117-0131 (in Russian)

[7] Nuriev S.A., Karcan I.N. Zashchishchennost' rechevoj informacii v nauchnyh organizaciyah ot utechki po tekhnicheskim kanalam. Sovremennye innovacii, sistemy i tekhnologii. 2023; 3(4): 0349-0362. https://doi.org/10.47813/2782-2818-2023-3-4-0349-0362 (in Russian)

[8] Nuriev S.A. SUBD v arhitekture GIS novogo pokoleniya. V sbornike: Voprosy kontrolya hozyajstvennoj deyatel'nosti i finansovogo audita, nacional'noj bezopasnosti, sistemnogo analiza i upravleniya. materialy VII Vserossijskoj nauchno-prakticheskoj konferencii. Moskva; 2022: 525-529. (in Russian)

[9] Petrenko A.S., Petrenko S.A., Kostyukov A.D., Ozhiganova M.I. Model' kvantovyh ugroz bezopasnosti dlya sovremennyh blokchejn-platform. Zashchita informacii. Insajd. 2022; 3(105): 10-20. (in Russian)

[10] Petrenko A.S., Petrenko S.A., Antonova-Druzhinina A.O., Ozhiganova M.I. Metod parametricheskogo vybora kriptoprimitivov dlya kvantovo-ustojchivoj blokchejn-platformy. CHast' I. Zashchita informacii. Insajd. 2022; 4(106): 24-33. (in Russian)

[11] Popov A.YU., Remez M.V., ZHilina E.V., Ozhiganova M.I. Parsing elektronnyh resursov. biblioteka selenium ili fake user agent? Informatizaciya v cifrovoj ekonomike. 2022; 4(3): 197-210. https://doi.org/10.18334/ide.3.4.115219 (in Russian)

[12] Ozhiganova M.I., SHejko A.O., Isakova E.M., Mironova A.O. Metody i sredstva provedeniya analiza ugroz lokal'noj vychislitel'noj seti predpriyatiya. V sbornike: Cifrovaya transformaciya nauki i obrazovaniya. Sbornik nauchnyh trudov II Mezhdunarodnoj nauchno-prakticheskoj konferencii. 2021: 264-270. (in Russian)

[13] Petrenko A.S., Petrenko S.A., Ozhiganova M.I. Ocenka vozmozhnostej kvantovyh algoritmov kriptoanaliza. Zashchita informacii. Insajd. 2021; 6(102): 70-82. (in Russian)

[14] Ozhiganova M.I., Kurtametov E.S. Primenenie mashinnogo obucheniya v zashchite veb-prilozhenij. NBI tekhnologii. 2020; 2(14): 16-20. https://doi.org/10.15688/NBIT.jvolsu.2020.2.3 (in Russian)

[15] Kalita A.O., Ozhiganova M.I., Tishchenko E.N. Osnovy organizacii adaptivnyh sistem zashchity informacii. NBI tekhnologii. 2019; 1(13): 11-15. https://doi.org/10.15688/NBIT.jvolsu.2019.1.2 (in Russian)

[16] Ozhiganova M.I., Kalita A.O., Tishchenko E.N. Postroenie adaptivnyh sistem zashchity informacii. NBI tekhnologii. 2019; 4(13): 12-21. https://doi.org/10.15688/NBIT.jvolsu.2019.4.2 (in Russian)

[17] Aver'yanov V.S., Karcan I.N. Metody ocenki zashchishchennosti avtomatizirovannyh sistem na baze kvantovyh tekhnologij soglasno CVSSV2.0/V3.1, Zashchita informacii. Insajd. 2023; 1(109): 18-23. (in Russian)

[18] Karcan I.N., ZHukov A.O. Mekhanizm zashchity promyshlennoj seti, Informacionnye i telekommunikacionnye tekhnologii, 2021; 52: 19-26. (in Russian)

ИНФОРМАЦИЯ ОБ АВТОРАХ / INFORMATION ABOUT THE AUTHORS

Карцан Игорь Николаевич, доктор технических наук, доцент, ведущий научный

Igor Kartsan, Dr. Sc., Docent, Leading Researcher, Marine Hydrophysical Institute,

сотрудник Морского гидрофизического института РАН, Севастополь, Россия
ORCID: 0000-0003-1833-4036

Russian Academy of Sciences, Sevastopol, Russia

Статья поступила в редакцию 05.06.2024; одобрена после рецензирования 10.06.2024; принята к публикации 12.06.2024.

The article was submitted 05.06.2024; approved after reviewing 10.06.2024; accepted for publication 12.06.2024.