Оригинальная статья / Original article

https://doi.org/10.21869/2223-1560-2020-24-2-136-152

Цифровые водяные знаки с адаптивной шириной информационного кольца в задаче скрытой передачи управляющего сигнала в многоагентной робототехнической системе

О.О. Шумская [1] ✉, А.О. Исхакова [2]

[1] Санкт-Петербургский Институт информатики и автоматизации Российской академии наук (СПИИРАН)
14 линия В.О. 39, г. Санкт-Петербург 199178, Российская Федерация

[2] ФГБУН «Институт проблем управления им. В.А. Трапезникова РАН»
ул. Профсоюзная 65, г. Москва 117997, Российская Федерация

✉ e-mail: shumskaya.oo@gmail.com

Резюме

Цель исследования. *Статья посвящена вопросу обеспечения безопасной передачи управляющих сигналов между элементами многоагентной робототехнической системы. Целью работы является обеспечение скрытой передачи данных с возможностью однозначного извлечения управляющих сигналов.*

Методы. *Для решения поставленной задачи был предложен алгоритм на основе методов водяных цифровых знаков и цифровой стеганографии. Метод формирования цифрового водяного в форме кольца с симметрией позволяет не только обеспечить максимальную незаметность встраивания (незначительные искажения контейнера при сокрытии), но и уберечь передаваемый сигнал от таких сложных искажений, как поворот изображения. Метод стеганографического сокрытия позволяет регулировать интенсивность встраивания с помощью фактора силы, вычислительно прост и понятен. Предложенный подход к выявлению и пониманию передаваемого сигнала отличается от современных методов криптографии и стегоанализа тем, что не требует 100% верного извлечения сигнала. После нескольких модификаций метод позволяет минимизировать времязатраты на формирование (адаптивная ширина кольца с битами сигнала) и встраивание цифрового водяного знака (минимизация обрабатываемой области контейнера для встраивания).*

Результаты. *Предложенный подход позволяет скрыто передать управляющие сигналы в рамках передачи цифровых объектов, эксперименты показали, что управляющий сигнал однозначно понимается даже при таких искажениях, как уменьшение или увеличение контрастности или яркости, поворот изображения, сжатие.*

Заключение. *Использование предложенной методики передачи управляющих сигналов в многоагентной робототехнической системе позволит своевременно и безопасно, с минимальной вероятностью потери, получать необходимую информацию.*

Ключевые слова: *многоагентная робототехническая система; робототехнические комплексы; взаимодействие роботов; управление роботами; информационная безопасность; стеганографические методы защиты информации; цифровой водяной знак; верификация.*

Конфликт интересов: *Авторы декларируют отсутствие явных и потенциальных конфликтов интересов, связанных с публикацией настоящей статьи.*

Финансирование. *Исследование выполнено при частичной финансовой поддержке РФФИ в рамках научного проекта № 19-01-00767.*

Для цитирования: Шумская О.О., Исхакова А.О. Цифровые водяные знаки с адаптивной шириной информационного кольца в задаче скрытой передачи управляющего сигнала в многоагентной робототехнической системе // *Известия Юго-Западного государственного университета.* 2020; 24(2): 136-152. https://doi.org/10.21869/2223-1560-2020-24-2-136-152.

Поступила в редакцию 30.01.2020 *Подписана в печать 19.02.2020* *Опубликована 20.04.2020*

Digital Watermarks with Adaptive Information Ring Width in the Issue of Hidden Transmission of a Control Signal in the Multi-Target Robotic System

Olga O. Shumskaya [1] ✉, Anastasia O. Iskhakova [2]

[1] St.Petersburg Institute for Informatics and Automation of the Russian Academy of Sciences (SPIIRAS)
39, 14-th Line V.O., St. Petersburg 199178, Russian Federation

[2] Institute of Control Science of RAS
65 Profsoyuznaya str., Moscow 117997, Russian Federation

✉ e-mail: shumskaya.oo@gmail.com

Abstract

Purpose of research. *The article is devoted to the issue of ensuring the safe transmission of control signals between the elements of a multi-agent robotic system. The purpose of the work is to provide hidden data transmission with the possibility of unambiguous extraction of control signals.*

Methods. *To solve the task set, an algorithm based on the methods of digital watermarks and digital steganography was proposed. The method of forming a digital watermark in the form of a ring with symmetry allows not only ensuring maximum imperceptibility of embedding (insignificant distortion of the container during concealment), but also to protect the transmitted signal from such complex distortions as image rotation. The steganographic concealment method allows regulating the intensity of embedding using the force factor; it is computationally simple and straightforward. The proposed approach to identifying and understanding the transmitted signal differs from modern methods of cryptography and steganalysis in that it does not require 100% correct signal extraction. After several modifications, the method allows minimizing the time spent on formation (adaptive width of the ring with signal bits) and embedding of a digital watermark (minimization of the processed area of the container for embedding).*

Results. *The proposed approach makes it possible to transmit control signals in a hidden way within the framework of the transmission of digital objects; the conducted experiments have shown that the control signal is unambiguously understood even with such distortions as a decrease or increase in contrast or brightness, image rotation, and compression.*

Conclusion. *Application of the proposed technique for transmitting control signals in a multi-agent robotic system will male it possible to receive the necessary information timely and safe, with a minimum probability of loss.*

Keywords: *multi-agent robotic system; robotic complexes; robot-robot interaction; robot control; IT security; steganographic methods.*

Conflict of interest*. The authors declare the absence of obvious and potential conflicts of interest related to the publication of this article.*

Funding. *The research was carried out with partial financial support of the RFBR in the framework of scientific project No. 19-01-00767.*

For citation: Shumskaya O. O., Iskhakova A. O. Digital Watermarks with Adaptive Information Ring Width in the Issue of Hidden Transmission of a Control Signal in the Multi-Target Robotic System. *Izvestiya Yugo-Zapadnogo gosudar-stvennogo universiteta = Proceedings of the Southwest State University*. 2020, 24(2): 136-152 (In Russ.). https:// doi.org/10.21869/2223-1560-2020-24-2-136-152.

Received 30.01.2020 *Accepted 19.02.2020* *Published 20.04.2020*

***

Введение

Актуальность разработки новых методов верификации агентов в мобильных робототехнических группах определена стремительным ростом распространения групповой робототехники в решении широкого спектра задач и в то же время отсутствием методического обеспечения для формирования безопасной среды обмена данными между агентами в таких группах. Актуальность разработки адаптированных алгоритмов маскирования управляющих сигналов связана со спецификой робототехнических комплексов, применяемых в силовых ведомствах (скрытие факта наличия роботов исполнителей, в условиях передачи потоков данных от роботов разведчиков) [1, 2].

В направлении робототехники сегодня актуальны задачи создания прорывных научно-технических решений, способных функционировать в условиях группового взаимодействия, создания сетецентрических систем управления, а также киберфизических систем комплексного назначения. Сетецентрическое управление подразумевает взаимодействия в группе типа «оператор-робот» и «робот-робот» («агент-агент»), тем самым характеризуя новый этап развития удаленной коммуникации между объектами, отличающийся наличием управляющих сигналов внутри группы и возможностью принятия решений агентами без участия оператора. Данная тенденция не только стала своего рода источником новых вызовов в области интеллектуализации систем управления, но и расширила спектр задач для разработчиков прикладных робототехнических комплексов, в том числе предназначенных для выполнения тактических задач. В этой связи прослеживается тенденция к популяризации комплексов групповой робототехники, увеличению числа роботов агентов в таких группах, и крайне важному аспекту – обеспечению их защищенного взаимодействия. Данная задача является комплексной и подразумевает решения целого множества научно-технических проблем, в том числе создания безопасных распределенных систем интеллектуального принятия решения на основе данных нескольких агентов, обеспечения целостности данных при взаимодействии (обмене данными) между агентами, а также конфиденциальности в условиях передачи информативных сигналов [3, 4].

Постановка задачи для системы защиты информации в многоагентных робототехнических комплексах, применяемых силовыми ведомствами, зачастую характеризуются необходимостью

учета таких условий, когда группа объектов (агентов) взаимодействует между собой вне зоны контролируемой территории. Данные обстоятельства накладывают ряд ограничений на открытую передачу данных и сигналов, поскольку в подобной обстановке вероятность несанкционированного доступа к данным и управлению агентами, а также связанные с этим риски, повышаются. В связи с изложенными особенностями возникает актуальная научная задача по модификации и адаптации применяемых для групп роботов методов защиты передаваемых данных и управляющих сигналов.

Материалы и методы

Текущее исследование предполагает решение фундаментальной проблемы создания эффективного обеспечения в области управления гетерогенными роботами и робототехническими комплексами, достижения необходимого уровня надежности и безопасности. Достижение данной цели предполагается за счет создания нового комплекса научно-технических решений для безопасного межмашинного обмена данными между агентами мобильных робототехнических групп с сетецентрическим управлением. Решение проблемы заключается в разработке концепции безопасного сетецентрического управления интеллектуальными роботами и коалициями роботов, создании соответствующих алгоритмов и протоколов безопасного взаимодействия, в частности реализации новых безопасных каналов передачи информации и интерфейсов взаимодействия с оператором / группой операторов / другими агентами [5, 6].

Рассмотрим группировку роботов в многоагентной системе в виде множества объектов C: $C = \{c_1, c_2, \ldots c_n\}$, где c_i – робототехническое автономное или частично автономное устройство, выполняющее частную тактическую задачу; $i = 1, \ldots, n$.

При этом каждое устройство c_i может быть охарактеризовано принадлежностью к одному из подмножеств множества C:

– принадлежность к подмножеству C^* наземной группы роботов, снабженных набором исполнительных устройств, предназначенных для выполнения общей цели, поставленной перед мобильной группировкой;

– принадлежность к подмножеству C'' – группы разведывательных роботов, в задачи которых входит выполнение обеспечивающих функций: разведка, координация и навигация множества роботов C^*.

Согласно описанной форме взаимодействия элементов группировки:

$C = C^* \cup C''$; $C^* \cap C'' = \varnothing$.

Также следует заметить, что радиус контролируемой территории определен некой территорией вокруг группировок – элементов описываемой среды. Также имеется комплекс контроля S, в задачи которого входят функции приема и передачи сигналов от элементов C_i друг к другу для обеспечения взаимодействия в рамках выполнения тактической задачи.

Рассредоточение роботов C_i по большому пространству, возможность перераспределения задач между агентами, а также увеличенный набор выполняемых задач за счет установки индивидуальных исполнительных устройств являются преимуществами такого распределения объектов группировки. Агенты - элементы подмножества *C''* обладают множеством демаскирующих признаков, которые делают их уязвимыми для охранных комплексов противника. При этом в общем представлении задачи предполагается, что ключи шифрования скомпрометированы, и противник может анализировать весь трафик, передаваемый между агентами разведки $c_i \in C''$. При этом, зачастую эффективным приемом таких проектов является наличие избыточности элементов в множестве *C"* с целью усложнения анализа противником выполняемой тактической операции. Следует отметит, что при такой формулировке задачи важным представляется сокрытие фактов наличия роботов множества *C** и передачи им управляющих сигналов от элементов множества *C''* и объекта *S*. Передача данных между элементами подмножеств *C** и *C''* с сокрытием факта обмена данными предполагается с применением современных методов криптографии и стеганографии, как объективно эффективных и прогрессивных методов в решении подобных задач [7, 8]. В частности, предлагается рассмотреть методы образования и передачи цифровых водяных знаков в видеопотоках между элементами $c_i \in C$ [9].

В качестве стегоконтейнера в рассматриваемом подходе выступает видеопоток, формируемый робототехнической группировкой агентов-разведчиков, который представляет собой последовательность цифровых изображений с изображением местности. Стеганография подразумевает встраивание любой информации максимально незаметно не только для человеческого глаза, но и для аналитических программ противников. Одним из важнейших факторов, обеспечивающих незаметное встраивание ЦВЗ, устойчивость к искажениям при формировании, хранении или передаче стегоконтейнера, является выбор области встраивания как самого ЦВЗ в исходный объект, так и информации в формируемый ЦВЗ. Современные подходы стеганографии уже давно ушли от идей встраивания какой-либо информации в пространственную область (значения пикселей), ученые отдают предпочтения частотной области, в частности все больше исследований касаются встраивания в коэффициенты дискретного преобразования Фурье (ДПФ). Такой выбор обоснован тем, что ДПФ позволяет вне зависимости от алгоритма встраивания достичь устойчивости от ряда атак [10, 11].

Общая схема таких алгоритмов сводится к нескольким основным шагам: формирование ЦВЗ на основе некоторого передаваемого сообщения согласно определенного правила; встраивание ЦВЗ в Фурье-образ; проверка наличия конкретного ЦВЗ в стегоконтейнере. Можно выделить еще одну

общую особенность всех подходов – параметр встраивания, характеризующий силу встраивания, иными словами, насколько значения ЦВЗ внесут искажения в коэффициенты ДПФ исходного изображения. Важно отметить, что порой даже незначительное искажение некоторых коэффициентов ДПФ может привести к явным артефактам или неестественным явлениям на цифровом объекте, поэтому значение такого параметра должно быть подобрано таким образом, чтобы ЦВЗ можно было бы обнаружить по необходимости, но при этом оставить его незаметным для злоумышленников.

Авторы [12] предлагают для встраивания использовать дайджест сообщения, полученный с помощью хэш-функции. Полученное таким образом сообщение путём операции XOR между парами приводят к размеру 80 битов, которые и будут является ЦВЗ.

Пространство сокрытия формируется из среднечастотных элементов первого и второго квадрантов Фурье-образа, значения которых на комплексной плоскости расположены в пределах кольцевой области заданной ширины. В данном случае фактор силы ЦВЗ не является параметром, он рассчитывается. Также рассчитываются разности между амплитудами симметрично расположенных элементов Фурье-образа. Встраивание осуществляется путём изменения амплитудных значений этих элементов.

Для обнаружения ЦВЗ рассчитывают долю верно извлечённых битов и сравнивают с пороговым значением. Если расчётное значение больше порога, то признаётся наличие ЦВЗ в изображении.

В работе [13] ЦВЗ формируется на основе псевдослучайно сгенерированного ключа. К полученному ЦВЗ применяют обратное логарифмическое полярное отображение, благодаря чему ЦВЗ приобретает свойство круговой симметрии. Это обеспечивает устойчивость перед геометрической атакой типа «поворот изображения». Процесс встраивания основан на пересчёте таких элементов амплитудного Фурье-спектра стегоконтейнера, которым соответствуют элементы цифрового водяного знака со значениями 1, путем усреднения по окрестности 3×3 с умножением на коэффициент усиления.

Для обнаружения факта встраивания искомого водяного знака авторы делят изображение на непересекающиеся окна размером 10×14 пикселей и ищут их локальные максимумы. Преобразуя локальные максимумы с помощью логарифмического полярного отображения, авторы определяют корреляцию между полученными значениями и значениями водяного знака. Решение о наличии ЦВЗ основывается на величине предопределенного порогового значения.

Автор работы [14] предполагает наличие ключа. Цифровое изображение делится на блоки 16×16 пикселей.

Встраивание осуществляется в среднечастотные элементы Фурье-образа, распределение битов ЦВЗ по которым осуществляется полуслучайным путем на основе ключа. Для извлечения ЦВЗ так же требуется знание ключа.

Авторы работы [15] предлагают циркулярное симметричное расположение битов сообщения в водяном знаке. ЦВЗ представляет собой амплитудный Фурье-спектр, элементы которого принимают значения из множества {-1, 1}. Элементы Фурье-образа образуют кольцо в области средних частот. Для устойчивости перед геометрической атакой типа «поворот изображения» ЦВЗ обладает симметрией: элементы зеркально отражены по диагонали. Авторами были рассмотрены два варианта встраивания: аддитивное и мультипликативное.

Для обнаружения наличия цифрового водяного знака в контейнере авторы предлагают рассчитывать корреляцию между значениями пикселей контейнера и предполагаемого ЦВЗ. Если величина корреляции превышает заранее предопределенный порог, то принимается решение о наличии проверяемого ЦВЗ в цифровом объекте.

Похожий алгоритм, но с меньшей емкостью водяного знака предложен авторами [16]. Емкость встраиваемого сообщения значительно сокращается из-за выбранной области в ЦВЗ. Авторы формируют ЦВЗ в виде окружности с оптимальным радиусом внедрения, а не кольца, и все элементы принимают значения из множества {0, 1}. В данном алгоритме встраивание в коэффициенты дискретного преобразования Фурье осуществляется аддитивно. Для того чтобы выявить наличие известного ЦВЗ в изображении, авторы используют алгоритм, обратный встраиванию, основанный на оценке корреляции между извлеченными значениями и значениями данного ЦВЗ. При увеличении значения корреляции более предопределенного порога принимается решение о наличии сокрытого ЦВЗ.

В алгоритме, предложенном авторами работы [17], пространство сокрытия формируется так же из среднечастотных элементов, однако только первого и второго квадрантов (верхняя половина) Фурье - образа, значения которых на комплексной плоскости расположены в пределах кольцевой области заданной ширины. Для встраивания одного бита секретного сообщения в зависимости от его значения изменяется пара симметрично расположенных элементов в первом и втором квадрантах так, чтобы разность между ними приняла соответствующее значение. При встраивании и обнаружении ЦВЗ алгоритм предполагает 2 секретных ключа: размеры стандартного изображения, к которым масштабируют исходное изображение, и величины радиусов, ограничивающих рассматриваемую кольцевую область.

Процесс выявления наличия предполагаемого ЦВЗ в изображении заключается в вычислении разности симметрично расположенных элементов в первом и втором квадрантах соответственно в пределах кольцевой области

заданной ширины. Если разность больше или равна 0, то значение бита ЦВЗ принимается равным 1, иначе 0. На основе процента верно определенных битов между предполагаемым ЦВЗ и только что извлеченным принимается решение: если выявлено соответствие более 75%, то считается, что данный ЦВЗ скрыт в изображении.

В работах [18, 19] по изображению–контейнеру перемещается окно размером 2×2. Встраивание является LSB-подобным, для записи битов сообщения используются младшие три бита частотных коэффициентов. В каждый блок встраивается 9 бит, во все элементы по 3 бита кроме DC-коэффициента.

Результаты и их обсуждение

Ниже приведен предлагаемый подход в виде алгоритмов преобразования сигнала в ЦВЗ, внедрения ЦВЗ и проверки наличия ЦВЗ.

Преобразование сигнала в ЦВЗ

Вход: Передаваемое сообщение, радиус R_{max} и граница R_{min}, определяющие ширину кольца встраивания; размеры ЦВЗ $N \times N$.

Выход: Сформированный ЦВЗ.

1. Преобразование сигнала в битовую последовательность.

2. Подбор значения R_{min} на основе длины битовой последовательности, но не менее его границы.

3. Расчет значений ЦВЗ согласно формуле

$$W(x,y) = \begin{cases} 0, R_{\max} < r < R_{\min} \\ \pm 1, R_{\min} < r < R_{\max} \end{cases}, \qquad (1)$$

где R_{min} и R_{max} – границы кольцевой области, $r = \sqrt{x^2 + y^2}$.

Ранее в алгоритм формирования ЦВЗ было добавлено условие на случай, если длина сообщения меньше емкости кольцевого пространства ЦВЗ. В таком случае генерировались случайные значения из множества {-1, 1}, что сводило к минимуму возможность создания второго подобного ЦВЗ, однако могло содержать большое количество лишней информации и увеличивать объем ЦВЗ.

Сейчас предлагается формировать кольцо адаптивной ширины на основе длины передаваемого сообщения. Это сокращает время формирования ЦВЗ, сам знак содержит больше полезной информации, что позволяет повысить устойчивость перед атаками, искажающими контейнер за счет того, что область полезной информации сокращена и более сконцентрирована. Однако, чтобы область концентрации информации находилась в средних частотах, значение R_{max} зафиксировано и равно 41, а R_{min} ограничено и не может быть менее 13. Кольцо с граничными значениями ширины позволяет вместить порядка 150 символов.

Формируемый ЦВЗ обладает свойством симметрии за счет зеркального отражения значений по диагонали.

Внедрение ЦВЗ

Вход: Цифровой водяной знак размером $N \times N$, цифровое изображение размером $M \times K$, фактор силы ЦВЗ a.

Выход: Стегоизображение размером $M \times K$.

Поскольку ДПФ и ОДПФ, применяемые к цифровому объекту для перехода в частотную область, увеличивают время затраты на вычисления с увеличением размерности самого объекта, а в задаче информирования роботов-исполнителей в сетецентрической системе каждая секунда на счету, то принято решение в процессе встраивания рассматривать центральный блок цифрового объекта размерами $2N \times 2N$. Поскольку блок встраивания больше ЦВЗ, то границы внесенных искажений будут достаточно размыты и незаметны, а скорость обработки стегоконтейнера увеличится в разы. Помимо повышения скорости встраивания это позволит повысить устойчивость к различным искажениям стегоизображения, так как доля информативного блока в общем изображении относительно мала и менее уязвима.

При встраивании новые амплитудные значения стегоконтейнера рассчитываются по формуле:

$$M'(x,y) = M(x,y) + aM(x,y)W(x,y), \quad (2)$$

где $M(x,y)$ – исходное амплитудное значение коэффициента ДПФ с координатами x, y.

В ходе работы были опробованы аддитивный и мультипликативный подходы внедрения ЦВЗ, было решено остановиться на мультипликативном, поскольку он позволял вносить меньшее искажение в контейнер при достаточном уровне обнаружения ЦВЗ.

Проверка наличия ЦВЗ

Вход: Стегоизображение размером $M \times N$, ЦВЗ размером $M \times N$, фактор силы ЦВЗ a, пороговое значение t.

Выход: Строка, содержащая решение о наличии искомого ЦВЗ в исследуемом стегоизображении.

1. Считывание стегоизображения, переход к цветовой модели YCbCr, дискретное преобразование Фурье (матрица F').

2. Считывание ЦВЗ, переход к виду -1, 0, 1 (матрица W).

3. Для каждого элемента из проверяемой области:

3.1. Если $W(x, y)=1$, то

3.1.1. прибавление к общей сумме Sum соответствующего элемента $F(x, y)$;

3.1.2. увеличение счетчика положительных элементов N_+ на единицу;

3.1.3. прибавление к сумме положительных элементов Sum_+ соответствующего элемента $F(x, y)$.

3.2. Иначе

3.2.1. прибавление к общей сумме Sum соответствующего элемента $F(x, y)$;

3.2.2. увеличение счетчика отрицательных элементов N_- на единицу;

3.2.3. прибавление к сумме отрицательных элементов Sum_- соответствующего элемента $F(x, y)$.

4. Вычисление корреляции по формуле:

$$C_n = \left(\frac{\sum\limits_{M'\in M'_+} M'(x,y)}{N_+} - \frac{\sum\limits_{M'\in M'_-} M'(x,y)}{N_-} \right) \frac{N_+ + N_-}{2\sum\limits_{M'\in M'_+} aM'(x,y)}, \quad (3)$$

где N_+ – количество элементов ЦВЗ, равных 1;

N_- – количество элементов ЦВЗ, равных -1.

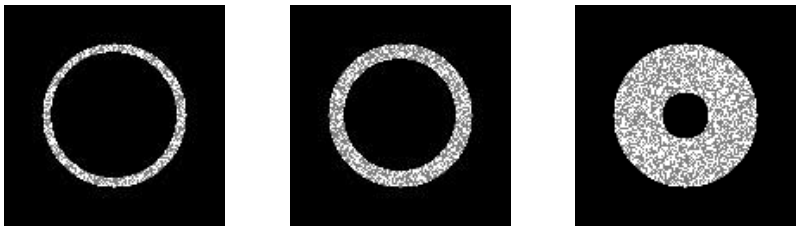
5. В случае если $C_n > T$, то принимается решение о наличии проверяемого ЦВЗ в стегоконтейнере, иначе – стегоконтейнер не содержит проверяемый ЦВЗ.

Для проверки эффективности предложенного подхода были проведены вычислительные эксперименты. В качестве контейнеров для проведения экспериментов были взяты фотографии неравномерной местности с различными препятствиями. Размер контейнеров 256×256 пикселей, сформированных ЦВЗ – 128×128. Вложение ЦВЗ в контейнер осуществляется в центральную часть контейнера таким образом, чтобы центр ЦВЗ совпадал с центром контейнера, если их размеры не совпадают. Симметричность формируемого ЦВЗ позволяет достигать устойчивости скрытых данных перед некоторыми атаками, поэтому, конечно, желательно, чтобы положение ЦВЗ оставалось неизменным, например, при поворотах контейнера на кратные 90° углы.

Пороговое значение C_n для всех тестов составляет 0,17. Радиус $R_2 = 41$, R_1 не менее 13, Фактор силы ЦВЗ $a = 0{,}3$.

Ниже представлены ЦВЗ, сформированные на основе секретных строк длинной 48 знаков (рис. 1.a), 77 знаков (рис. 1.b) и 150 знаков (рис. 1.c). При варьировании параметров емкость ЦВЗ достигает 2 300 знаков, однако в таком случае кольцо занимает практически весь ЦВЗ.

Далее в таблицах приведены результаты экспериментов: исходный контейнер, встраиваемый ЦВЗ, стегоконтейнер после встраивания, применяемая атака, результаты проверки наличия искомого ЦВЗ в контейнере. Приведенные в табл.2 и табл.3 результаты вычислительных экспериментов с применением искажений передаваемых стегоизображений, содержащих скрытый управляющий сигнал, показали, что даже довольно существенное изменение яркости и/или контрастности объекта не препятствует корректному распознаванию сигнала.



a) **b**) **c**)

Рис. 1. Сформированные ЦВЗ

Fig. 1. Formed DWTs

Таблица 1. Вычислительные эксперименты без реализации атак

Table 1. Computational experiments without atacks

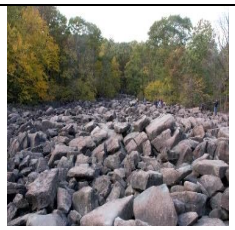
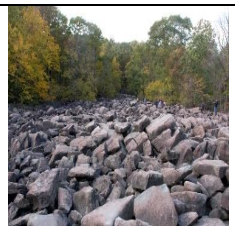
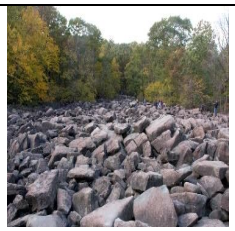
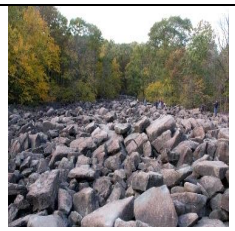
Исходное изображение			
Встроенный ЦВЗ	без вложения	с	
Стегоизображение			
Атака	без атаки	без атаки	
Проверяемый ЦВЗ	a	c	a
C_n	0,0378	0,6771	0,0013
Проверяемый ЦВЗ найден?	Нет	Да	Нет

Таблица 2. Вычислительные эксперименты с искажением стегоизображения

Table 2. Computational experiments with stego-image deformation

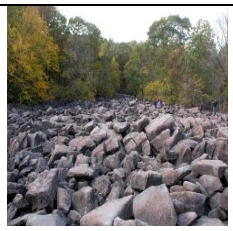
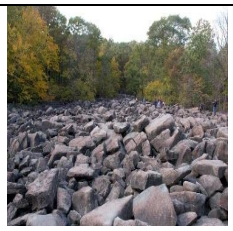
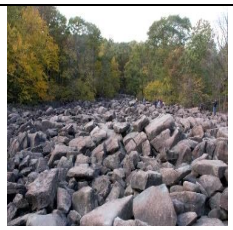
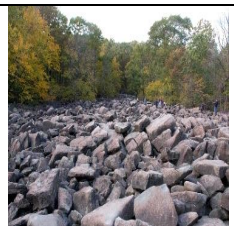
Исходные данные	Исходное изображение			Встроенный ЦВЗ		Стегоизображение			
				b					
Атака	JPEG-сжатие	Изменение яркости, %				Изменение контрастности, %			
		-40	-20	+20	+40	-40	-20	+20	+40
Проверяемый ЦВЗ	b								
C_n	0,2570	0,2187	0,3513	0,4435	0,3965	0,3871	0,4119	0,4497	0,4290
Проверяемый ЦВЗ найден?	Да								

Таблица 3. Вычислительные эксперименты с атакой «поворот изображения»

Table 3. Computational experiments with image rotation atack

Исходные данные	Исходное изображение	Встроенный ЦВЗ	Стегоизображение
		с	
Атака	Поворот на 9°	Поворот на 60°	Поворот на 180°
Проверяемый ЦВЗ	с		
C_n	0,3020	0,0833	0,6771
Проверяемый ЦВЗ найден?	Да	Нет	Да

А величины корреляций, превышающие пороговое значение с запасом, позволяют сделать вывод, что метод устойчив и к более значительным искажениям.

В то же время реализация атак «Поворот изображения» позволило проверить степень защиты при различных вариантах искажения: при повороте на 9 градусов, 60 градусов и 180 градусов и показало, что распознавание управляющего сигнала не осуществилось при 60-градусном повороте. Это объясняется алгоритмом встраивания ЦВЗ, который основан на последовательном распределении бит в четырех сегментах изображения, часть из которых оказывается «обрезанными» при повороте более чем на 15 градусов в любую из сторон. Таким образом, можно сделать вывод, что метод устойчив к искажениям изображений путем поворота на 0-15, 165-195, 345-375 градусов из-за потери значительной части изображения в иных случаях, то есть потери самой передаваемой информации. Эксперимент с JPEG-сжатием объекта показал также устойчивость подхода к такой атаке. Атака злоумышленника, результатом которой является потеря передаваемого изображения, легко обнаруживается на начальных этапах и не может оказаться незамеченной. Для решения такой проблемы должны применяться дополнительные средства противодействия атакам. При это можно констатировать, что предлагаемый метод устойчив к рассмотренным атакам для решения поставленных задач маскирования управляющих сигналов агентов в мобильных робототехнических группах с сетецентрическим управлением даже при частичной потере или искажении части передаваемой информации.

Выводы

В современной прикладной робототехнике эффективного решения многих задач возможно достичь только при групповом взаимодействии роботов [20]. Предложенный подход и основанный на нем алгоритм позволяют скрыть факт передачи управляемых сигналов робототехническим системам. Опубликованные в статье результаты проведенных экспериментальных вычислений позволяют сделать вывод об устойчивости предлагаемого подхода перед преднамеренными сторонними атаками на передаваемые сигналы, а также перед случайными возможными искажениями при обмене данными. Преимуществом алгоритма перед аналогичными алгоритмами криптографии или классической стеганографии является и тот факт, что нет необходимости на 100% корректного извлечения встроенных данных, в то время как в методах криптографии и классической стеганографии каждый бит информации крайне важен для распознавания конечного сигнала [21]. Описанный в статье подход позволил повысить скорость формирования ЦВЗ за счет адаптивной ширины информативного кольца, повысить скорость обработки стегоконтейнера и встраивания ЦВЗ благодаря обработке части объекта, снизить вносимые искажения в стегоизображение, относительно предыдущих исследований [22]. Предложенный подход и полученные результаты могут быть использованы для формирования защищенных механизмов межмашинного обмена данными между агентами в групповых робототехнических системах.

Список литературы

1. Будко П.А., Виноградeнко А.М., Литвинов А.И. Реконфигурация каналов связи при управлении смешанными группировками робототехнических комплексов // Известия ЮФУ. Технические науки. 2017. №2 (187). С. 266–278.

2. Подходы к формированию единого информационного-управляющего поля смешанных робототехнических группировок / А.С. Сигов, В.В. Нечаев, В.В. Баранюк, О.С. Смирнова // Современные информационные технологии и ИТ-образование. 2016. №1. С. 146–151.

3. The cybersecurity in development of IoT embedded technologies / B. Usmonov, O. Evsutin, A. Iskhakov, A. Shelupanov, A. Iskhakova, R. Meshcheryakov // Proceedings of the International Conference on Information Science and Communications Technologies (ICISCT, 2017). 2017. P. 1–4. https://doi.org/10.1109/ICISCT.2017.8188589.

4. Использование тепловой карты поведения пользователя в задаче идентификации субъекта инцидента информационной безопасности / А. Ю. Исхаков, А. О. Исхакова, Р. В. Мещеряков, Р. Бендрау, О. Мелехова // Труды СПИИРАН. 2018. № 6 (61). С. 147-171. https://doi.org/10.15622/sp.61.6.

5. Зикратов И.А., Козлова Е.В., Зикратова Т.В. Анализ уязвимостей робототехнических комплексов с роевым интеллектом. Научно-технический вестник информационных технологий, механики и оптики. 2013. №5 (87). С. 149–154.

6. Method of Verification of Robotic Group Agents in the Conditions of Communication Facility Suppression / A. Iskhakova, A.Iskhakov, R. Meshcheryakov, E. Jharko // IFAC-PapersOnLine. 2019. Vol. 52, no. 13. P. 1397-1402. https://doi.org/10.1016/j.ifacol.2019.11.394

7. Конахович Г.Ф. Компьютерная стеганография. Теория и практика. Киев: МК-Пресс, 2006. 288 с.

8. Евсютин О.О., Кокурина А.С., Мещеряков Р.В. Обзор методов встраивания информации в цифровые объекты для обеспечения безопасности в «интернете вещей» // Компьютерная оптика. 2019. Т. 43. № 1. С. 137–154. https://doi.org/ 10.18287/2412-6179-2019-43-1-137-154.

9. Федосеев В.А. Цифровые водяные знаки и стеганография. Самара: СГАУ, 2015. 128 с.

10. Евсютин О.О., Кокурина А.С., Мещеряков Р.В. Стеганографическое встраивание дополнительных данных в снимки дистанционного зондирования земли с помощью метода QIM с переменным шагом квантования в частотной области // Известия Томского политехнического университета. Инжиниринг георесурсов. 2019. Т. 330, № 8. С. 155–162. https://doi.org/10.18799/24131830/ 2019/8/2221.

11. Подход к извлечению робастного водяного знака из изображений, содержащих текст / А. В. Козачок, С. А. Копылов, Р. В. Мещеряков, О. О. Евсютин, Л.М. Туан // Труды СПИИРАН. 2018. № 5(60), С. 128-155. https://doi.org/10.15622/sp.60.5.

12. Robust Watermarking Method in DFT Domain for Effective Management of Medical Imaging / M. Cedillo-Hernandez, F. Garcia-Ugalde, M. Nakano-Miyatake, H. Perez-Meana // Signal, Image and Video Processing. 2015. Vol. 9. P.1163–1178.

13. Ridzon R., Levicky D. Content Protection in Grayscale and Color Images Based on Robust Digital Watermarking // Telecommunication Systems. 2013. Vol. 52. P.1617–1631.

14. Gaata M. T. An Efficient Image Watermarking Approach based on Fourier Transform // International Journal of Computer Applications. 2016. Vol. 136(9). P.8–11.

15. Шумская О.О., Будков В.Ю. Сравнительное исследование методов классификации в стегоанализе цифровых изображений // Научный вестник НГТУ. 2018. № 3 (72). С. 121–134. https://doi.org/10.17212/1814-1196-2018-3-121-134.

16. Solachidis V., Pitas I. Circularly Symmetric Watermark Embedding in 2-D DFT Domain // IEEE Transactions on Image Processing. 2001. Vol. 10. P. 1741–1753.

17. Poljicak A., Mandic L., Agic D. Discrete Fourier Transform-based Watermarking Method with an Optimal Implementation Radius // Journal of Electronic Imaging. 2011. Vol. 20. P. 033008-1–033008-8.

18. Mandal J.K., Khamrui A. A Genetic Algorithm Based Steganography in Frequency Domain (GASFD // International Conference on Communication and Industrial Application. 2011. P. 1–4.

19. Image Data Hiding Technique Using Discrete Fourier Transformation / D. Bhattacharyya, T. Kim, H. Adeli, R.J. Robles, M. Balitanas // Communications in computer and information science. 2011. Vol. 151. P. 315–323.

20. Ронжин А.Л., Юсупов Р.М. Многомодальные интерфейсы автономных мобильных робототехнических комплексов // Известия ЮФУ. Технические науки. 2015. № 1 (162). С. 195–206.

21. Шумская О.О., Железны М. Адаптивный алгоритм встраивания информации в сжатые JPEG-изображения на основе операции замены // Информационно-управляющие системы. 2018. № 5. С. 44–56. https://doi.org/ 10.31799/1684-8853-2018-5-44-56.

22. Shumskaya O.O., and Iskhakova A.O. Application of digital watermarks in the problem of operating signal hidden transfer in multi-agent robotic system // 2019 International Siberian Conference on Control and Communications (SIBCON). 2019. https:// doi.org/10.1109/SIBCON.2019.8729669.

References

1. Budko P.A., Vinogradenko A.M., Litvinov A.I. Rekonfiguratsiya kanalov svyazi pri upravlenii smeshannymi gruppirovkami robototekhnicheskikh kompleksov [Reconfiguration of communication channels during control of mixed groups of robotic complexes]. *Izvestiya YuFU. Tekhnicheskie nauki = Izvestiya SFedU. Engineering Sciences*, 2017, no. 2 (187), pp. 266–278 (In Russ.).

2. Sigov A.S., Netchaev V.V., Barabyuk V.V., Smirnova O.S. Podkhody k formirovaniyu edinogo informatsionnogo-upravlyayushchego polya smeshannykh robototekhnicheskikh gruppirovok [Approaches to formation of single information and control field of mixed robotics groupings]. *Sovremennye informatsionnye tekhnologii i IT-obrazovanie = Modern Information Technology and IT-education.* 2016. no.1, pp. 146–151 (In Russ.).

3. Usmonov B., Evsutin O., Iskhakov A., Shelupanov A., Iskhakova A., Meshcheryakov R. The cybersecurity in development of IoT embedded technologies. *Proceedings of the International Conference on Information Science and Communications Technologies (ICISCT, 2017)*, 2017, pp. 1–4. https://doi.org/10.1109/ICISCT.2017.8188589.

4. Iskhakov A. Y., Iskhakova A. O., Meshcheryakov R. V., Bendraou R., Melekhova O. Ispol'zovanie teplovoi karty povedeniya pol'zovatelya v zadache identifikatsii sub"ekta intsidenta informatsionnoi bezopasnosti [Application of User Behavior Thermal Maps for Identification of Information Security Incident]. *Trudy SPIIRAN = SPIIRAS Proceedings*, 2018, no. 6(61), pp. 147-171. https://doi.org/10.15622/sp.61.6 (In Russ.).

5. Zikratov I.A., Kozlova E.V., Zikratova T.V. Analiz uyazvimostei robototekhnicheskikh kompleksov s roevym intellektom [Analysis of vulnerabilities of robotic complexes with Swarm intelligence*]. Nauchno-tekhnicheskii vestnik informatsionnykh tekhnologii,*

mekhaniki i optiki = Scientific and Technical Journal of Information Technologies, Mechanics and Optics, 2013, no.5 (87), pp. 149–154 (In Russ.).

6. Iskhakova A., Iskhakov A., Meshcheryakov R., Jharko E. Method of Verification of Robotic Group Agents in the Conditions of Communication Facility Suppression. *IFAC-PapersOnLine*, 2019, vol. 52, no. 13, pp. 1397-1402. https://doi.org/10.1016/j.ifacol.2019.11.394

7. Konahovitch G.F. Komp'yuternaya steganografiya [Computer steganography]. *Teoriya i praktika = Theory and Practice*. Kiev, MK-Press Publ., 2006, 288 p. (In Russ.).

8. Evsyutin O.O., Kokurina A.S., Meshcheryakov R.V. Obzor metodov vstraivaniya informatsii v tsifrovye ob"ekty dlya obespecheniya bezopasnosti v «internete veshchei» [A review of the methods of embedding information in digital objects for security in the Internet of things]. *Komp'yuternaya optika = Computer Optics*. 2019, vol. 43(1), pp. 137–154. https://doi.org/10.18287/2412-6179-2019-43-1-137-154 (In Russ.).

9. Fedoseev V.A. *Tsifrovye vodyanye znaki i steganografiya* [Digital watermarks and steganography]. Samara, SSAU Publ., 2015, 128 p. (In Russ.).

10. Evsyutin O.O., Kokurina A.S., Meshcheryakov R.V. Steganograficheskoe vstraivanie dopolnitel'nykh dannykh v snimki distantsionnogo zondirovaniya zemli s pomoshch'yu metoda QIM s peremennym shagom kvantovaniya v chastotnoi oblasti [Steganographic embedding of additional data into the images of earth remote sensing by QIM method with a variable quantization step in the frequency domain]. *Izvestiya Tomskogo politekhnicheskogo universiteta. Inzhiniring georesursov = Bulletin of the Tomsk Polytechnic University. Geo Assets Engineering*, 2019, vol. 330. 8, pp. 155–162. https://doi.org/10.18799/24131830/2019/8/2221 (In Russ.).

11. Kozachok A.V., Kopylov S.A., Meshcheryakov R.V., Evsutin O.O., Tuan L.M. Podkhod k izvlecheniyu robastnogo vodyanogo znaka iz izobrazhenii, soderzhashchikh tekst [An approach to a robust watermark extraction from images containing text]. *Trudy SPIIRAN = SPIIRAS Proceedings*, 2018, vol. 5(60), pp. 128-155. https://doi.org/10.15622/sp.60.5. (In Russ.).

12. Cedillo-Hernandez M., Garcia-Ugalde F., Nakano-Miyatake M., and Perez-Meana H. Robust Watermarking Method in DFT Domain for Effective Management of Medical Imaging. *Signal, Image and Video Processing*, 2015, vol. 9, pp.1163–1178.

13. Ridzon R., and Levicky D. Content Protection in Grayscale and Color Images Based on Robust Digital Watermarking. *Telecommunication Systems*, 2013, vol. 52, pp.1617–1631.

14. Gaata M. T. An Efficient Image Watermarking Approach based on Fourier Transform. *International Journal of Computer Applications*, 2016, vol. 136(9), pp.8–11.

15. Shumskaya O.O., Budkov V.Yu. Sravnitel'noe issledovanie metodov klassifikatsii v stegoanalize tsifrovykh izobrazhenii [Comparative study of classification methods in the stegoanalysis of digital images]. *Nauchnyi vestnik NGTU = Science Bulletin of the Novosibirsk State Technical University*. 2018, vol. 3 (72), pp. 121–134. https://doi.org/10.17212/1814-1196-2018-3-121-134 (In Russ.).

16. Solachidis V., and Pitas I. Circularly Symmetric Watermark Embedding in 2-D DFT Domain. *IEEE Transactions on Image Processing*, 2001, vol. 10, pp. 1741–1753.

17. Poljicak A., Mandic L., and Agic D. Discrete Fourier Transform-based Watermarking Method with an Optimal Implementation Radius. *Journal of Electronic Imaging*, 2011, vol. 20, pp. 033008-1–033008-8.

18. Mandal J.K., Khamrui A. A Genetic Algorithm Based Steganography in Frequency Domain (GASFD. *International Conference on Communication and Industrial Application*, 2011, pp. 1–4.

19. Bhattacharyya D., Kim T., Adeli H., Robles R.J., and Balitanas M. Image Data Hiding Technique Using Discrete Fourier Transformation. *Communications in Computer and Information Science*, 2011, vol. 151, pp. 315–323.

20. Ronzhin A.L., Yusupov R.M. Mnogomodal'nye interfeisy avtonomnykh mobil'nykh robototekhnicheskikh kompleksov [Multi-modal interfaces of autonomous mobile robotics systems]. *Izvestiya YuFU. Tekhnicheskie nauki = Izvestiya SFedU. Engineering Sciences*, 2015, no. 1 (162), pp. 195–206 (In Russ.)

21. Shumskaya O.O., Zelezny M. Adaptivnyi algoritm vstraivaniya informatsii v szhatye JPEG-izobrazheniya na osnove operatsii zameny [Adaptive algorithm of replacement-based embedding of data into compressed JPEG images]. *Informatsionno-upravlyayushchie sistemy = Information and Control Systems*, 2018, vol. 5, pp. 44–56. https://doi.org/10.31799/1684-8853-2018-5-44-56 (In Russ.)

22. Shumskaya O.O., and Iskhakova A.O. Application of digital watermarks in the problem of operating signal hidden transfer in multi-agent robotic system. *2019 International Siberian Conference on Control and Communications (SIBCON)*. 2019. doi: 10.1109/ SIBCON.2019.8729669.

Информация об авторах / Information about the Authors

Шумская Ольга Олеговна, аспирант, Санкт-Петербургский институт информатики и автоматизации Российской академии наук, г. Санкт-Петербург, Российская Федерация, e-mail: shumskaya.oo@gmail.com

Olga O. Shumskaya, Post-Graduate Student, St. Petersburg Institute for Informatics and Automation of the Russian Academy of Sciences, St. Petersburg, Russian Federation, e-mail: shumskaya.oo@gmail.com

Исхакова Анастасия Олеговна, кандидат технических наук, старший научный сотрудник, лаборатория киберфизических систем, Федеральное государственное бюджетное учреждение науки «Институт проблем управления им. В.А. Трапезникова РАН», г. Москва, Российская Федерация, e-mail: iskhakova.ao@gmail.com

Anastasia O. Iskhakova, Cand. of Sci. (Engineering), Associate Professor Senior Researcher, Cyberphysical Systems Laboratory, Russian Academy of Sciences, Institute of Management Problems named after V.A. Trapeznikova RAS, Moscow, Russian Federation, e-mail: iskhakova.ao@gmail.com