Применение цифровых водяных знаков в задаче скрытой передачи управляющего сигнала в многоагентной робототехнической системе

О.О. Шумская,
м.н.с., shumskaya.oo@gmail.com
СПИИРАН, г. Санкт-Петербург
А.О. Исхакова,
с.н.с. ИПУ РАН, г. Москва

Авторами рассматривается актуальная задача разработки концепции безопасного управления интеллектуальными роботами и коалицией роботов. Такие робототехнические комплексы имеют широкий спектр применения, в том числе они используются для разведывательных и спасательных задач. Создание соответствующих алгоритмов и протоколов защищенного взаимодействия позволит решить задачи создания единого подхода к управлению робототехническими комплексами, а также повышения эффективности данного процесса. В настоящей статье представлен предлагаемый подход сокрытия управляющих сигналов, алгоритмическое обеспечение и данные о вычислительных экспериментах, направленные на формирование механизмов защищенного взаимодействия между агентами робототехнической системы, основанный на применении стеганографических методов для сокрытия управляющих сигналов.

The relevant problem of development of the concept of safe control of intelligent robots and coalition of robots is considered by authors. Such robotic complexes have a wide range of application, including they are used for prospecting and rescue tasks. Creation of the corresponding algorithms and protocols of the protected interaction will allow to solve problems of creation of uniform approach to management of robotic complexes and also increases in efficiency of this process. In this article are provided the offered approach, algorithmic providing and data of computing experiments directed to forming of mechanisms of the protected interaction between agents of robotic system based on application of steganographic methods for concealment of managing signals.

1. Актуальность решаемой задачи

Робототехнические комплексы, включая военные, транспортные, образовательные, бытовые, индивидуальные, находят применение в различных сферах человеческой деятельности. При решении разведывательных, а также тактических задач высокую эффективность показывают методы группового применения мобильных роботов [1, 2]. Робототехнические группы, в основе управления которыми лежит сетецентрическая система, отличаются повышенной достоверностью, своевременностью и точностью информации.

При реализации групповых систем приоритетной задачей становится решение проблемы формирования защищенных механизмов межмашинного обмена данными между роботами, коммуникации между которыми осуществляются вне зоны контролируемой территории. Существующие подходы по обеспечению защиты информации в таких системах не могут быть применены для экстремальных условий такого приоритетного направления как робототехника в связи с массовой интеграцией специфических технологий, а также отсутствием адаптированных моделей угроз и моделей нарушителя [3]. В работе раскрывается предлагаемый подход сокрытия управляющих сигналов, алгоритмическое обеспечение и данные о вычислительных экспериментах, направленные на формирование механизмов защищенного взаимодействия между агентами робототехнической системы, основанный на применении стеганографических методов для сокрытия управляющих сигналов. Предполагается, что стеганографическая защита передаваемых сигналов с помощью цифровых водяных знаков позволит осуществлять безопасную передачу критических данных между роботами внутри сети вне контролируемой зоны.

2. Характеристика объекта исследования

В рамках раскрытия концепции исследуемой проблемы авторами приводится краткое описание примера частной задачи. Под исходной задачей будем понимать выполнение некоторой операции с привлечением робототехнической группировки.

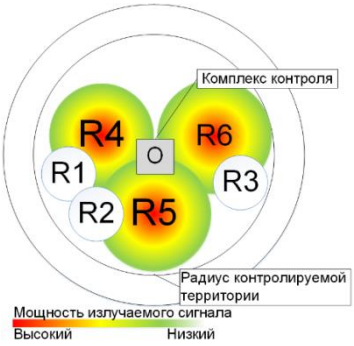


рис. 1 Схема коммуникации между субъектами многоагентной системы

На рисунке 1 приведена схема коммуникации между субъектами многоагентной системы. Основным исполнителем тактической задачи является наземная подгруппа роботов R1-R3. Они снабжены ограниченным

набором исполнительных устройств, предназначенных для выполнения общей цели, поставленной перед мобильной группировкой. В обязанности агентов R4-R7 входит выполнение обеспечивающих функций (разведка, координация и навигация подгруппы R1-R3). Учитывая экстремальные условия среды и вероятную автономность группировки, агенты R4-R7 должны быть обеспечены не только различными наборами сенсоров, но и мощными вычислителями, предназначенными для интеллектуального анализа разведывательных данных и оперативного принятия решений о необходимости отправки управляющих сигналов группировке R1-R3.

Преимущества такого подхода очевидны: рассредоточение роботов по большому пространству, возможность перераспределения задач в случае поломки или выхода из строя в экстремальных условиях, расширенный набор выполняемых функций, достигаемых за счет установки на каждого агента индивидуальных исполнительных устройств.

В качестве исходной посылки предположим, что агенты группировки R4-R6 обладают множеством демаскирующих признаков, которые делают их уязвимыми для охранных комплексов противника. Кроме того, будем полагать, что ключи шифрования скомпрометированы и противник может анализировать весь трафик, передаваемый между агентами разведки. При этом, зачастую эффективным приемом таких проектов является наличие избыточности в группировке R4-R7 с целью усложнения анализа противником выполняемой тактической операции.

В подобных условиях важным представляется сокрытие факта наличия группировки R1-R3. В связи с тем, что результатом дистанционной разведки как правило является видеосъёмка местности, авторами предпринята попытка сокрытия передачи управляющих сигналов в цифровом видеопотоке для R1-R3 с применением современных методов стеганографии. Под направлением стеганографии понимаются методы сокрытия секретной информации, позволяющие сделать неочевидным для злоумышленника сам факт её наличия [4]. В частности, далее приводятся результаты эксперимента по распознаванию управляющих сигналов с помощью аппарата цифровых водяных знаков (далее – ЦВЗ). Изначально, данная технология была предназначена для защиты авторских прав на мультимедийные объекты. Выделяют следующие категории ЦВЗ [5]:

- хрупкие – неустойчивые перед какими-либо искажениями контейнера;
- полухрупкие – устойчивые перед определенным набором искажений контейнера;
- робастные – устойчивы даже перед частичной утерей контейнера.

Цифровые водяные знаки можно разместить как поверх объекта, так и скрыть его посредством методов стеганографического встраивания.

3. Стеганографическая защита передаваемых сигналов с помощью ЦВЗ

Для того чтобы обеспечивать незаметность встраивания ЦВЗ и устойчивость к искажениям, возникающим при формировании, хранении и передаче цифрового объекта, необходимо выбрать область сокрытия в цифровом объекте. В данной работе в качестве стегоконтейнера рассматривается видеопоток, получаемый с робототехнической группировки агентов-разведчиков. Видеопоток представляет собой последовательный набор цифровых изображений. Встраивание в частотную область изображения, а именно дискретное преобразование Фурье позволяют добиться устойчивости к ряду атак за счёт своих свойств вне зависимости от конкретного алгоритма встраивания.

Все подобные алгоритмы построены по общей схеме: сначала необходимо сгенерировать ЦВЗ из исходной информации по определённому правилу, затем встроить его в Фурье-образ, а впоследствии проверить наличие ЦВЗ в изображении с некоторой заданной долей вероятности. Также общим для всех алгоритмов является наличие некоторого параметра встраивания, характеризующего силу встраивания.

В работе [6] рассмотрено циркулярное симметричное вложение водяного знака. Авторы предлагают формировать цифровой водяной знак с помощью псевдослучайной ключевой последовательности в виде амплитудного Фурье-спектра, значения элементов которого принадлежат множеству {–1, 1}. Элементы Фурье-образа образуют кольцо в области средних частот. Круговая симметрия генерируемой ЦВЗ обеспечивает устойчивость перед геометрической атакой «поворот изображения». Авторами были рассмотрены два варианта встраивания: аддитивное и мультипликативное.

Процесс выявления наличия цифрового водяного знака в стегоконтейнере осуществляется с помощью вычисления корреляции между предполагаемым водяным знаком и изображением, в котором, возможно, скрыт этот водяной знак. Если полученное значение превышает заданное пороговое значение, то принимается решение, что в изображение встроен искомый ЦВЗ.

Схожий алгоритм описан в [7], однако авторы формируют ЦВЗ в виде окружности с оптимальным радиусом внедрения, а не кольца, и все элементы принимают значения из множества {0, 1}. Авторы рассмотрели аддитивное встраивание в коэффициенты дискретного преобразования Фурье.

Чтобы определить наличие конкретного водяного знака в изображении, авторы используют обратный встраиванию алгоритм, и находят корреляцию между извлеченными значениями и значениями предполагаемого водяного знака. В случае если величина корреляции превышает предопределенный порог, авторы принимают решение, что искомый ЦВЗ скрыт в данном изображении.

В алгоритме, предложенном авторами работы [8], 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 работе [9] ЦВЗ формируется на основе псевдослучайно сгенерированного ключа. Для устойчивости перед геометрической атакой типа «поворот изображения» к ЦВЗ применяют обратное логарифмическое полярное отображение, благодаря чему ЦВЗ приобретает свойство круговой симметрии. 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 порога.

Автор работы [10] 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.

В работах [11, 12] 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.

4. Защита передаваемых сигналов

4.1. Преобразование сигнала в ЦВЗ

Вход: Строка, содержащая сигнал; радиусы R_{min} и R_{max}, ограничивающие ширину кольца встраивания; размеры ЦВЗ M×N.

Выход: Сформированный ЦВЗ.

Расчет значений ЦВЗ осуществляется согласно формуле:

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

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

Стоит отметить, что в алгоритм формирования ЦВЗ было добавлено условие на случай, если длина сообщения меньше емкости кольцевого пространства ЦВЗ. В таком случае генерируются случайные значения из множества {-1, 1}, что сводит к минимуму возможность создания второго подобного ЦВЗ.

4.2. Внедрение ЦВЗ

Вход: Цифровой водяной знак размером M×N, цифровое изображение размером M×N, фактор силы ЦВЗ a.

Выход: Стегоизображение размером M×N.

При встраивании новые амплитудные значения рассчитываются по формуле:

$$M'(x,y) = \begin{cases} M(x,y) + aW(x,y), \textit{аддитивное}, \\ M(x,y) + aM(x,y)W(x,y), \textit{мультипликативное}, \end{cases} \quad (2)$$

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

В качестве способа встраивания был выбран мультипликативный способ.

4.3. Проверка наличия ЦВЗ

Вход: Стегоизображение размером M×N, ЦВЗ размером M×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 YC_bC_r, 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:

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

где N_+ – количество элементов ЦВЗ, равных 1,

N_-– количество элементов ЦВЗ, равных -1.

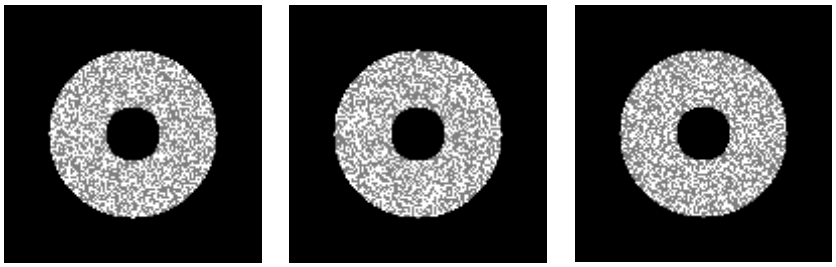
5. Если $C_n > T$, то принимается решение о наличии проверяемого ЦВЗ в стегоконтейнере, иначе – стегоконтейнер не содержит проверяемый ЦВЗ.

5. Вычислительные эксперименты

В качестве контейнеров для проведения экспериментов были взяты фотографии территории парка, как пример неравномерной местности с различными препятствиями. Размер контейнеров 256×256 пикселей, а сформированных ЦВЗ – 128×128. Если размеры ЦВЗ не совпадают с размерами контейнера, то вложение осуществляется в центральную часть контейнера таким образом, чтобы центр ЦВЗ совпадал с центром контейнера. Симметричность формируемого ЦВЗ позволяет достигать устойчивости скрытых данных перед некоторыми атаками, однако важно, чтобы положение ЦВЗ оставалось неизменным, например, при поворотах контейнера на кратные 90° углы.

Пороговое значение C_n для всех тестов составляет 0,17. Радиусы: R_1 = 13, R_2 = 41. Фактор силы ЦВЗ a = 0,3.

Ниже представлены ЦВЗ, сформированные на основе секретных строк длинной 48 знаков (рис. 2.a), 77 знаков (рис. 2.b) и 300 знаков (рис. 2.c). При варьировании параметров емкость ЦВЗ достигает 2 300 знаков.



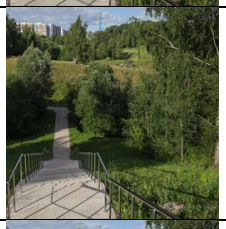
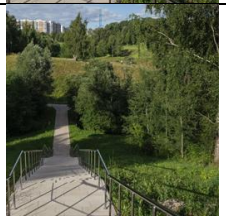
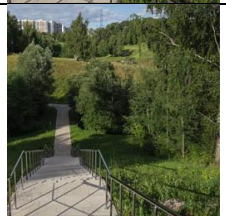
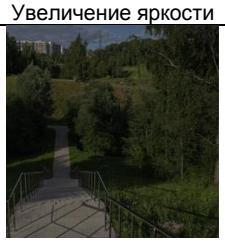
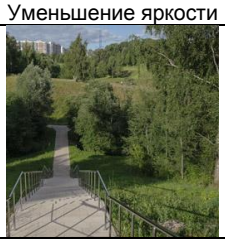
a) b) c)

рис. 2 Сформированные ЦВЗ

Ниже приведенырезультаты экспериментов: исходный контейнер, встраиваемый ЦВЗ, стегоконтейнер после встраивание и после некоторой атаки, результаты проверки наличия искомого ЦВЗ в контейнере.

Таблица 1

Вычислительные эксперименты

Исходное изображение	Встроенный ЦВЗ	Стегоизображение	Стегоконтейнер после атаки	Проверяемый ЦВЗ	C_n	Найден проверяемый ЦВЗ?
	без вложения		без атаки	a	0,0250	Нет
	c		без атаки	c	0,4520	Да
				a	0,0008	Нет
	b		 Увеличение яркости	b	0,4024	Да
	b		 Уменьшение яркости	b	0,2172	Да
	b			b	0,4355	Да

			Уменьшение контрастности			
	с		 Поворот на 3°	с	0,3752	Да
	с		 Поворот на 180°	с	0,4958	Да

Вывод

В современной прикладной робототехнике эффективного решения многих задач возможно достичь только при групповом взаимодействии роботов [13]. 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. Предложенный подход и полученные результаты могут быть использованы для формирования защищенных механизмов межмашинного обмена данными между агентами в групповых робототехнических системах.

Литература

1. Будко П.А., Виноградено 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. Сигов А.С., Нечаев В.В., Баранюк В.В., Смирнова О.С. Подходы к формированию единого информационного-управляющего поля смешанных робототехнических группировок // Современные информационные технологии и ИТ-образование. – 2016. – №1. – С. 146-151.
3. Зикратов Игорь Алексеевич, Козлова Екатерина Владимировна, Зикратова Татьяна Викторовна Анализ уязвимостей робототехнических комплексов с роевым интеллектом // Научно-технический вестник информационных технологий, механики и оптики. – 2013. – №5 (87). – С. 149-154.
4. Конахович Г.Ф. Компьютерная стеганография. Теория и практика. / Г.Ф. Конахович, А.Ю. Пузыренко. – К.: МК-Пресс, 2006. – 288 с.
5. В.А. Федосеев Цифровые водяные знаки и стеганография: учебное пособие с заданиями для практических и лабораторных работ // Самара: СГАУ, 2015. – 128 с.
6. Solachidis, V. Circularly Symmetric Watermark Embedding in 2-D DFT Domain / V. Solachidis, I. Pitas // IEEE Transactions on Image Processing. –2001. – Vol. 10. – P.1741–1753.
7. Poljicak A. Discrete Fourier Transform-based Watermarking Method with an Optimal Implementation Radius / A. Poljicak, L. Mandic, D. Agic // Journal of Electronic Imaging. – 2011. – Vol. 20. – P.033008-1–033008-8.
8. Cedillo-Hernandez M. 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.
9. Ridzon, R. Content Protection in Grayscale and Color Images Based on Robust Digital Watermarking / R. Ridzon, D. Levicky // Telecommunication Systems. – 2013. – Vol. 52. – P.1617–1631.
10. Gaata, Methaq T. An Efficient Image Watermarking Approach based on Fourier Transform / Methaq T. Gaata // International Journal of Computer Applications. – 2016. – Vol. 136. – No. 9. – P.8–11.
11. Mandal, J.K. A Genetic Algorithm Based Steganography in Frequency Domain (GASFD) / J.K. Mandal, A. Khamrui // International Conference on Communication and Industrial Application. – 2011. – P.1–4.
12. Bhattacharyya, D. 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.
13. Ронжин А.Л., Юсупов Р.М. Многомодальные интерфейсы автономных мобильных робототехнических комплексов// Известия ЮФУ. Технические науки.– 2015. – № 1 (162). – С. 195-206.