ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ТЕЛЕКОММУНИКАЦИИ
INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS

УДК 004.056
DOI: 10.21822/2073-6185-2022-49-4-113-125 Оригинальная статья /Original Paper

Метод стеганодетектирования скрытых изображений для систем защиты объектов интеллектуальной собственности

Ф.Б. Тебуева, М.Г. Огур, И.В. Мандрица, А.Б. Чернышев, Г.И. Линец, В.П. Мочалов
Северо-Кавказский федеральный университет,
355017, г. Ставрополь, ул. Пушкина, 1, Россия

Резюме. Цель. Целью исследования является повышение качества обнаружения и стеганодетектирования скрытых изображений, внедряемых в защищаемый объект интеллектуальной собственности различными методами. **Метод.** Предлагается метод стеганодетектирования скрытых изображений на основе глубокого обучения. Метод основан на использовании модели сверточной нейронной сети VGG16, в которой произведена оптимизация архитектуры и параметров обучения. **Результат.** Повышение точности обнаружения изображений-стегоконтейнеров на 3,8 %, а также возможность использования алгоритма разработанного метода для изображений, имеющих большее разрешение, чем размерность входа искусственной нейронной сети. **Вывод.** Разработанный метод предназначен для проведения стеганодетектирования в двух случаях: для выявления факта незаконного использования объектов интеллектуальной собственности; для применения в компьютерной криминалистике при идентификации изображений, содержащих скрытую и запрещенную к распространению информацию.

Ключевые слова: стеганодетектирование скрытых изображений, глубокое обучение, искусственная нейронная сеть

Для цитирования: Ф.Б. Тебуева, М.Г. Огур, И.В. Мандрица, А.Б. Чернышев, Г.И. Линец, В.П. Мочалов. Метод стеганодетектирования скрытых изображений для систем защиты объектов интеллектуальной собственности. Вестник Дагестанского государственного технического университета. Технические науки. 2022; 49(4):113-125. DOI:10.21822/2073-6185-2022-49-4-113-125

Stegan detection method for latent images for intellectual property protection systems

F.B. Tebueva, M.G. Ogur, I.V. Mandritsa, A.B. Chernyshev, G.I. Linets, V.P. Mochalov
North-Caucasus Federal University,
1 Pushkina Str., Stavropol 355017, Russia

Abstract. Objective. Improving the quality of detection and stego-detection of latent images embedded in the protected object of intellectual property by various methods. **Method.** The method for stego-detection of latent images based on deep learning is proposed. The method is based on the use of the VGG16 convolutional neural network model, in which the architecture and training parameters are optimized. **Result.** Increasing the accuracy of detecting stegocontainer images by 3.8%, as well as the possibility of using the algorithm of the developed method for images with a higher resolution than the dimension of the input of an artificial neural network. **Conclusion.** The developed method is intended for stegan detection in two cases: to detect the fact of illegal use of intellectual property objects; for use in computer forensics when identifying images containing hidden and prohibited information.

Keywords: hidden image stegan detection, deep learning, artificial neural network

For citation: F.B. Tebueva, M.G. Ogur, I.V. Mandritsa, A.B. Chernyshev, G.I. Linets, V.P. Mochalov. Stegan detection method for latent images for intellectual property protection systems. Herald of the Daghestan State Technical University. Technical Science. 2022; 49(4):113-125. DOI:10.21822/2073-6185-2022-49-4-113-125

Введение. В цифровом мире стеганодетектирование изображений и видео по-прежнему является относительно новой областью цифровых технологий и представляет собой раздел

компьютерной криминалистики. Каждый день пользователь сталкивается с огромным количеством изображения и видео, и среди них могут быть и те, в которые встроены секретные данные для проведения киберпреступлений.

Для оценки современного состояния научно-технического прогресса в области стеганодетектирования цифровых изображений и медиафайлов в настоящей статье проведено исследование научных публикаций по существующим методам. Так, в статье [1] представлен обзор и анализ различных существующих методов стеганографии, а также некоторые общие стандарты и рекомендации, взятые из литературы.

В статье [2] представлен обзор стеганографии и стеганодетектирования цифровых изображений, в основном охватывающий фундаментальные концепции, прогресс в области стеганографических методов для изображений в формате JPEG, а также вопросы разработки соответствующих стеганалитических схем. Приведены вопросы повышения эффективности стеганографических методов и возможности улучшения технологий стеганодетектирования. В статье [3] исследуется состояние стеганографии и стеганодетектирования с точки зрения текущих тенденций. Приведены современные методы стеганографии и стеаганодетекции (изображения и видео), которые встречаются в литературе последних лет. Так же анализируется набор данных и инструменты, доступные для мультимедийной стеганографии и стеганодетектирования, с примерами практического использования.

Самый простым методом стеганографии является встраивание сообщения после конца файла (end of file, EOF), либо помещение скрытой информации в заголовок EXIF, содержащий дополнительные сведения об изображении. Оба метода просты и быстры, но уязвимы для стеганодетектирования. Даже при обычном просмотре файла с помощью шестнадцатеричного редактора, сообщение, если оно не зашифровано, может быть обнаружено. Однако, поскольку такие сообщения легко могут быть обнаружены, были разработаны как новые методы стеганографии, рассмотренные ранее в данной работе, так и новые методы стеганодетектирования, направленные на противодействие им.

В зависимости от метода атаки, который использует стегоаналитика, можно выделить шесть основных категорий методов стеганодетектирования:

- визуальное стеганодетектирование;
- сигнатурное стеганодетектирование;
- статистическое стеганодетектирование;
- стеганодетектирование методом расширения спектра;
- стеганодетектирование в области преобразований;
- универсальное стеганодетектирование.

Рассмотрим более подробно каждую из групп.

Визуальное стеганодетектирование является одним из простейших способов стеганодетектирования. Визуальная атака на стегоконтейнер состоит в изучении подозрительного изображения невооруженным глазом для выявления любых заметных искажений. На практике такая задача оказывается очень трудной, поскольку изменения, внесенные в изображение при встраивании сообщения, как правило, не приводят к заметному ухудшению качества. Большинство стеганографических алгоритмов создают на выходе объект, слабо отличающийся от исходного пустого стегоконтейнера. Однако при удалении неизмененных частей стегоизображения можно наблюдать признаки манипуляции. Следовательно, если аналитик может идентифицировать те особенности изображения, которые характеризуют его как заполненный стегоконтейнер, визуальная атака может выявить существование скрытого сообщения.

Наиболее распространенной формой визуального стеганодетектирования является анализ наименьшего значащего бита (НЗБ). Изображение преобразуется в двоичную форму, после чего из него извлекаются младшие биты цветовых каналов. В цветовых каналах изображений обычно содержится одинаковое количество четных и нечетных значений. Иначе говоря, единиц в младших битах должно быть примерно столько же, сколько нулей. Однако при преобразова-

нии текста в двоичный формат данное статистическое свойство может нарушаться. Это вызывает визуальную несогласованность и помогает аналитику классифицировать изображение как заполненный стегоконтейнер. Однако данный метод успешен только тогда, когда для формирования стегоизображения использовался «плохой» стеганографический алгоритм.

Типичными программными средствами, использующими подход НЗВ, являются Camouflage и JpegX [4, 5] – ранние стеганографические программы, которые в настоящее время устарели и используются реже из-за простоты их обнаружения [6]. Их «плохой» алгоритм помещает биты сообщения в младшие биты цветовых каналов без какой-либо предварительной обработки. Менее вероятна ситуация, когда имеется доступ к исходным изображениям (пустым стегоконтейнерам). Тогда изображения с подозрением на наличие стегопосылки сравниваются с соответствующими исходными изображениями.

Еще одним признаком существования скрытых сообщений могут являться пустые места в изображениях. Их наличие может быть связано с тем, что некоторые стеганографические алгоритмы обрезают или дополняют изображение так, чтобы оно соответствовало фиксированному размеру. Различия в размере файла между пустым контейнером и изображением со стегопосылкой, увеличение или уменьшение числа уникальных цветов в изображениях также могут быть использованы в качестве индикаторов скрытых сообщений.

Метод определения стеганографического содержания в изображениях JPEG независимо от сигнатуры инструмента предложен в работах [7, 8]. Данный метод заключается в том, что изображение делится на блоки 8×8 пикселей, после чего для каждого блока путем анализа значений коэффициентов дискретного косинусного преобразования определяется матрица квантования. Затем матрица квантования сравнивается на предмет совместимости со стандартной матрицей квантования JPEG. Если есть несовместимые блоки, изображение характеризуется как заполненный стегоконтейнер.

Статистическое стеганодетектирование основано на использовании подходов, разработанных в результате исследования влияния встраивания данных на статистические характеристики сообщения, такие как коэффициенты корреляции, энтропия, параметры распределений, вероятности появления элементов и т.д.

Для достижения максимальной точности стеганодетектирования необходимо глубокое понимание процесса встраивания скрытого сообщения. Стеганографические алгоритмы, работающие в пространственной области, применяются непосредственно к пикселям изображения.

Такие алгоритмы делятся на две основные категории: замена НЗБ и сопоставление НЗБ. При замене НЗБ наименее значимые биты байтов изображения-контейнера заменяются секретными данными. В алгоритмах замены НЗБ существуют две схемы встраивания: последовательная и рандомизированная. Последовательное встраивание означает, что алгоритм начинает работу с первого пикселя изображения-контейнера и внедряет биты данных сообщения по порядку, пока не будет встроено все сообщение. При рандомизированном встраивании пиксели для встраивания выбираются по некоторой более сложной схеме.

Рассмотрим методы стеганодетектирования, направленные на выявление встраивания скрытых сообщений методом замены LSB. Вестфельд и Пфицманн [9] предложили первый метод статистического стеганодетектирования. Этот метод обнаруживает пары значений, измененных в результате встраивания сообщения. Причем пары содержат элементы, отличающиеся младшим битом. Они могут быть значениями яркости, коэффициентами дискретного косинусного преобразования (ДКП) или индексами палитры. Вестфельд и Пфицманн утверждают, что частоты появления каждого отдельного значения из каждой такой пары имеют тенденцию значительно отличаться от среднего значения их частот появления. Таким образом, с помощью критерия хи-квадрат можно обнаружить несоответствие реального распределения теоретическому, и, следовательно, выявить факт внедрения скрытой информации. Метод хи-квадрат надежно обнаруживает последовательно встраиваемые сообщения, но малоэффективен при рандомизированном встраивании. Для такого типа встраивания существует более общая реали-

зация атаки хи-квадрат [10, 11]. Для решения задач статистического стеганодетектирования активно используются подходы, основанные на машинном обучении. Так, в работе [12] для классификации изображений-контейнеров на пустые и заполненные используются деревья решений и ИНС. Авторы статьи [13] использовали для выявления факта внедрения скрытого сообщения авторегрессионную модель и классификатор, основанный на методе опорных векторов (SVM), а также несколько параметров регрессии для прогнозирования длины скрытой информации. Фридрих и др. [14] предложили детектор на основе машинного обучения, использующий в качестве признаков факты одновременное появление соседних шумовых остатков.

В статье [15] предложены две альтернативные схемы стеганодетектирования для стеганографии с расширенным спектром. Первая схема использует методы регрессии для оценки изображения-контейнера и стегоизображения. Для обнаружения секретного сообщения оценочное значение вычитается из стегоизображения. Вторая схема использует статистические методы более высокого порядка. Эксперименты показали, что в сравнении с первой предложенной схемой использование статистики более высокого порядка позволило повысить результативность стеганодетектирования.

Универсальное стеганодетектирование направлено на обнаружение скрытых сообщений вне зависимости от того, какой стеганографический метод был применен к изображению. Основная трудность разработки таких методов состоит в поиске общих черт, характерных для стегоизображений. В рамках данного подхода наибольшее применение находят методы машинного обучения.

В работе [16] в целях построения статистических характеристик высокого порядка для естественных изображений применяется вейвлет-разложение. Для различения нетронутых и измененных изображений используется линейный дискриминантный анализ Фишера. По результатам экспериментов, точность метода варьируется от 1,3% до 94% в зависимости от стеганографического алгоритма и длины сообщения (от 32 × 32 до 256 × 256). Данная работа демонстрирует сложность создания метода, показывающего высокую эффективность при противодействии широкому классу стеганографических методов.

Авторы работы [17] также использовали вейвлет-подобную декомпозицию для построения статистических моделей естественных изображений. Для различения пустых и заполненных изображений-контейнеров в работе использован метод опорных векторов. В [18] теми же исследователями предложено расширение модели для цветных изображений. Для упрощения процесса обучения классификатора был использован одноклассовый метод опорных векторов.

В работе [19] представлен метод стеганодетектирования для противодействия последовательной стеганографии. Для оценки положения и длины сообщения используются резкие изменения в статистических характеристиках изображения. Эти изменения являются характерной особенностью, которая отличает последовательную стеганографию от других типов.

В исследовании [20] предложено стеганодетектирование на основе сверточных нейронных серей. Предлагаемая сеть имеет структуру, отличную от искуственной нейронной сети, разработанной для задач компьютерного зрения. Вместо случайной инициализации веса в первом слое сети инициализируются базовым набором высокочастотных фильтров, используемым при вычислении остаточных карт. Кроме того, в модели используется новая функция активации, называемая усеченным линейным блоком. Производительность стеганодетектирования была повышена за счет включения информации о канале выбора. Этот подход оказался способным с высокой точностью обнаруживать несколько современных стеганографических схем в пространственной области для широкого диапазона размеров полезных нагрузок (0,05-0,5 бит на пиксель).

Постановка задачи. Учитывая результаты проведённого обзора существующих методов стеганодетектирования, можно сделать вывод, что в качестве основы разрабатываемого метода следует использовать технологии глубокого обучения искусственной нейронной сети (ИНС), поскольку в настоящее время они позволяют добиться наибольшей универсальности в распо-

знавании стегоконтейнеров, заполненных с применением различных стеганографических алгоритмов. Однако разработка ИНС сопряжена с рядом сложностей. В частности, выбор архитектуры ИНС для решения конкретной задачи значительно влияет на эффективность полученного решения. Например, одиночный нейрон способен воспринимать и воспроизводить прямую в мерном пространстве.

Более сложные сети могут описывать более сложные структуры, но проблема состоит в том, чтобы определить, какая сеть наиболее точно и полно соответствует структуре задачи. Целью разработчика ИНС является создание сети, достаточно сложной для обработки требуемых данных, но достаточно маленькой, чтобы избежать переобучения.

ИНС могут быть обучены численному решению задач, но ошибочный выбор размера и структуры сети способен привести к значительной потере эффективности. В частности, сеть, имеющая слишком малый размер по количеству нейронов или количеству скрытых слоев, будет иметь тенденцию изучать наиболее грубые взаимосвязи в обучающих данных и игнорировать более тонкие детали, что является критичным с точки зрения стеганодетектирования. Однако слишком большая сеть будет иметь тенденцию чрезмерно специализироваться и слишком хорошо «запоминать» обучающую выборку, и, как следствие, иметь плохие обобщающие способности.

Основная задача стеганодетектирования изображений состоит в определении факта наличия или отсутствия в некотором входном изображении скрытого сообщения. По своей сути данная задача является задачей бинарной классификации, т.к. предполагает отнесение объекта к одному из двух классов. Наибольшую эффективность в решении подобных задач в настоящее время демонстрируют сверточные нейронные сети.

Методы исследования. В качестве основы предлагаемого метода стеганодетектирования используется ИНС с архитектурой VGG-16 (рис. 1), которая была изначально разработана для классификации изображений, однако хорошо себя зарекомендовала и в ряде других областей, связанных с обработкой изображений.

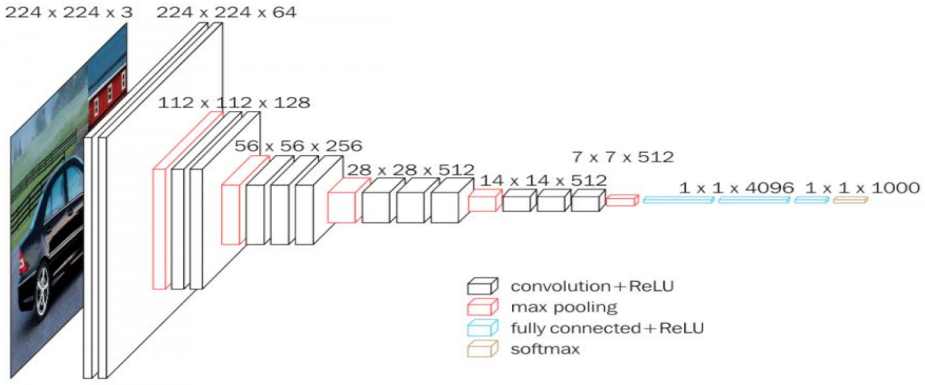

Рис.1. Структура оригинальной ИНС VGG-16
Fig.1. Structure of the original ANN VGG-16

Для решения задач стеганодетектирования в архитектуру ИНС внесены изменения:

– размер входного изображения изменён на 256x256;

– во всех сверточных блоках, начиная со второго, применяется пространственное исключение (spatial dropout) с вероятностью 0,1;

– функция активации в сверточных блоках изменена с ReLU на Leaky ReLU;

– в сверточных блоках после применения функции активации добавлен слой получения абсолютного значения (ABS);

– после слоя ABS в сверточные блоки добавлен слой пакетной нормализации (batch normalization, BN);

– полносвязная часть сети заменена на структуру, изображённую на рис. 2,а;

– в качестве оптимизатора использован стохастический градиентный спуск (SGD).

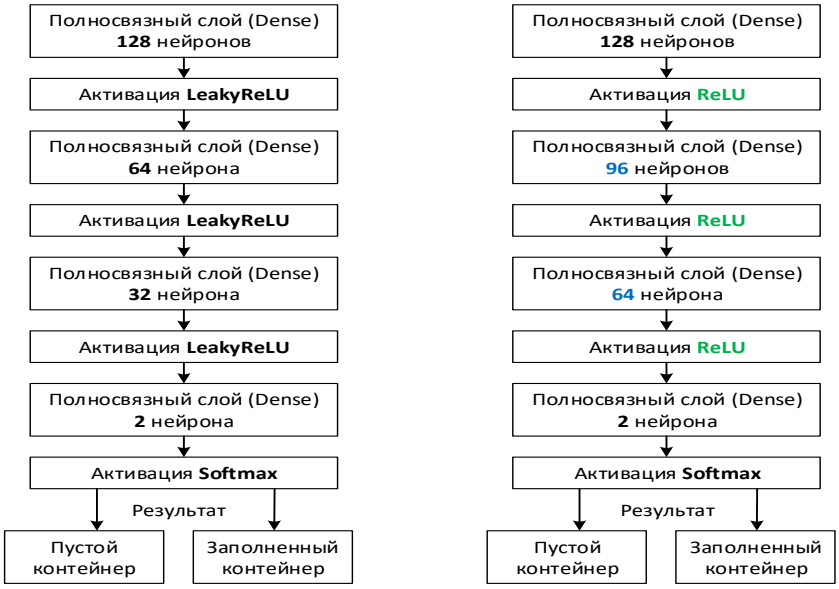

Рис.2. Исходная (а) и модифицированная (б) структура полносвязной части ИНС для проведения стеганодетектирования
Fig.2. Initial (a) and modified (b) structure of the full-link part of the ANN for steganodetection

В рамках предлагаемого метода стеганодетектирования структура полносвязной части сети заменена структурой, изображенной на рис. 2,б: функция активации заменена на ReLU, во втором и третьем полносвязных слоях количество нейронов увеличено с 64 до 96 и с 32 до 64 соответственно. Обучение ИНС предлагается выполнить с использованием языка программирования Python 3.8 и библиотеки TensorFlow версии 2.2.

В качестве обучающей выборки использованы изображения из библиотек BOSSBase и BOWS 2, в общей сложности 20 тысяч пар изображений. Все изображения приведены к размеру 256x256 пикселей, после чего в них внедрены стеганографические нагрузки с помощью алгоритма S-UNIWARD с плотностью упаковки 0,4 бит/пиксель. 14000 пар изображений использованы для обучения, 1000 пар для валидации, 5000 пар для тестирования. Гиперпараметры обучения, использованные в оригинальном и предлагаемом методе, представлены в табл. 1.

Таблица 1. Гиперпараметры обучения ИНС
Table 1. Hyperparameters of ANN training

Гиперпараметр Hyperparameter	**Метод-аналог Analogue method**	**Предлагаемый метод Proposed method**
Инициализатор свёрточных и полносвязных слоёв Initializer for Convolutional and Fully Connected Layers	Glorot Normal	
Вероятность пространственного исключения (spatial dropout)	0,1	
Оптимизатор Optimizer	SGD с моментом 0,95	
Коэффициент скорости обучения (learning rate)	0,005	0,003
Размер пакета (batch size)	64	32

Графики обучения ИНС в соответствии с методом-аналогом и предлагаемым методом представлены на рис. 3 и 4.

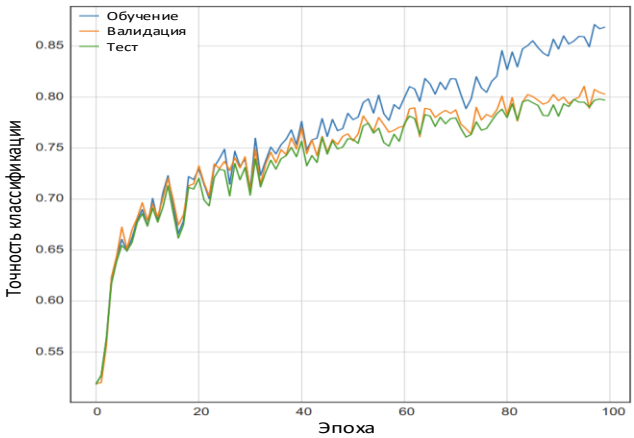

Рис.3. Точность классификации в зависимости от эпохи обучения для метода-аналога
Fig.3. Classification accuracy as a function of training epoch for the analogue method

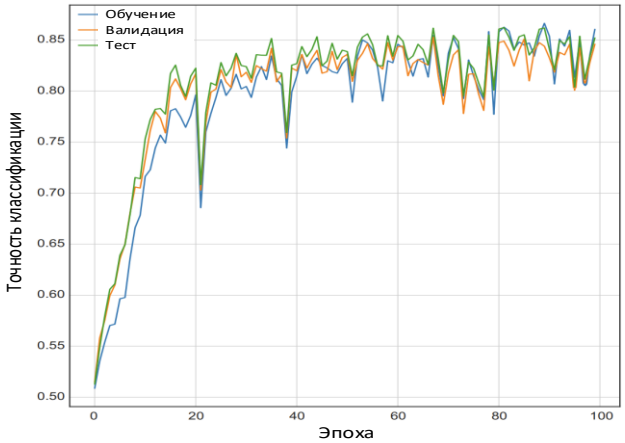

Рис.4. Точность классификации в зависимости от эпохи обучения для предлагаемого метода
Fig.4. Classification accuracy as a function of the epoch of learning for the proposed method

Итоговая точность классификации изображений на предмет наличия встроенного сообщения методом-аналогом составила 0,812. Точность классификации, достигаемая предлагаемым методом, составила 0,843. При этом в случае метода-аналога на последних эпохах наблюдаются признаки начала переобучения.

В качестве метрики точности распознавания стегоконтейнеров предлагается использовать метрику BinaryAccuracy, вычисляемую по правилу:

$$BinaryAccuracy = \frac{1}{N}\sum_{i=1}^{N}\begin{cases} 1, & \text{если } a_i' = a_i \ \wedge \ b' = b_i \\ 0 & \text{в противном случае} \end{cases}, \qquad (1)$$

где N – число изображений в выборке;

a_i – величина, равная единице, если -е изображение является пустым контейнером, и нулю в противном случае;

b_i – величина, равная единице, если -е изображение является заполненным стегоконтейнером, и нулю в противном случае;

a_i' – величина, равная единице, если первый выход ИНС принимает значение больше порогового при подаче на вход ИНС -го изображения, и нулю в противном случае;

b_i' – величина, равная единице, если второй выход ИНС принимает значение больше порогового при подаче на вход ИНС -го изображения, и нулю в противном случае. Величина порогового значения составляла 0,5.

В результате внесения изменений в структуру полносвязной части ИНС, а также изменения параметров обучения удалось добиться повышения точности обнаружения изображений-стегоконтейнеров на 3,8 %. Стоит отметить, что в настоящее время отсутствуют универсальные

методики определения структуры ИНС и гиперпараметров обучения, которые были бы оптимальными для решения задач определённого класса. Их выбор во многом зависит от интуиции разработчика и производится эмпирически. Таким образом, возможно дальнейшее совершенствование предложенного метода за счёт оптимизации структуры ИНС и модификации процесса обучения.

Обсуждение результатов. Основным недостатком предлагаемого подхода к стеганодетектированию изображений в его текущем виде является фиксированный размер входного изображения (в данном случае – 256x256 точек). В общем случае изображение-стегоконтейнер может иметь произвольное разрешение, в т.ч. с иным соотношением сторон. Предварительное масштабирование изображения до необходимого размера не является оптимальным подходом, поскольку по своей сути является разрушающим воздействием по отношению к скрытому сообщению. Если входное изображение имеет по крайней мере по одной из сторон большее количество пикселей, чем размерность входа ИНС, уменьшение размера изображения приведёт к потере информации и ухудшит качество детектирования. Если изображение имеет меньшие размеры, то увеличение изображения до размерности входа также может привести к непредсказуемым результатам ввиду применения интерполяции.

Для адаптации метода стеганодетектирования к изображениям произвольного размера может быть использовано разбиение входного изображения на сегменты, имеющие размер, соответствующий размерности входа ИНС. Если изображение имеет разрешение, не кратное размеру входного блока, предлагается произвести двух- или четырёхкратное разбиение изображения с различным положением начального блока (рис. 5).

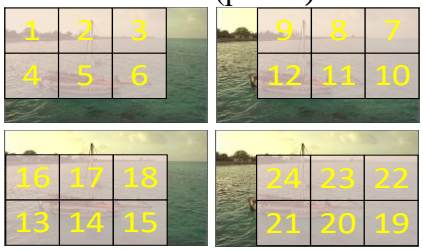

Рис.5. Пример разбиения изображения произвольного размера на блоки фиксированного размера

Fig.5. Example of splitting an arbitrary-sized image into fixed-sized blocks

Хотя такой подход приводит к увеличению вычислительной нагрузки, он позволяет избежать применения каких-либо механизмов выравнивания (дополнение нулями, дополнение другим фрагментом изображения и т.п.), результатом работы которых могут быть нетипичные для обученной ИНС входные данные.

В результате применения такого подхода для каждого блока изображения ИНС формирует метрики его принадлежности к одному из двух классов. Решение о наличии скрытого сообщения в изображении принимается следующим образом: если по крайней мере для одного блока изображения значение на втором выходе ИНС превышает некоторый порог разграничения $p_{min} \in (0; 1)$, данное изображение классифицируется как стегоконтейнер.

Значение величины p_{min} следует выбрать таким образом, чтобы минимизировать количество ошибок первого и второго рода.

Под ошибкой первого рода понимается определение пустого контейнера как изображения со скрытым сообщением. Ошибка второго рода – определение заполненного стегоконтейнера как изображения, не содержащего скрытых сообщений. Определение значения p_{min} произведено экспериментально. Для проведения эксперимента с сайта unsplash.com взяты 2000 изображений. В половину из них внедрены скрытые сообщения с использованием алгоритма S-UNIWARD с плотностью упаковки 0,4 бит/пиксель, после чего проведено их распознавание с помощью предложенного метода при различных значениях p_{min}. Для каждого значения p_{min} измерено количество ошибок первого и второго рода, а также общее число ошибок (рис. 6).

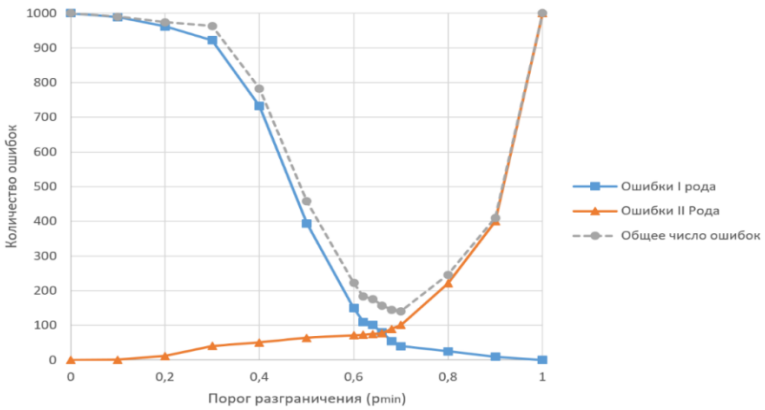

Рис.6. Зависимость количества ошибок распознавания стегоконтейнеров от порога разграничения
Fig.6. Dependence of the number of recognition errors of stegocontainers on the delimitation threshold

Исходя из результатов эксперимента, наилучшие результаты достигаются при p_{min} в интервале $[0{,}6; 0{,}7]$. Наименьший общий процент ошибок (14,1 %) достигается при значении $p_{min} = 0{,}7$, однако данное значение может быть неоптимальным, если принять, что ошибки первого и второго рода имеют различный вес. Поскольку использованная в рамках экспериментов ИНС обучена с применением лишь одного типа стеганографического алгоритма (S-UNIWARD), она в текущем виде не рассчитана на практическое применение для обнаружения широкого класса стегоконтейнеров.

Однако результаты экспериментов со стегоконтейнерами, полученными в результате простой замены наименьших значащих бит изображения псевдослучайной последовательностью, демонстрируют уровень обнаружения порядка 82%, хотя в обучающей выборке отсутствовали изображения подобного типа. Этот факт является дополнительным подтверждением эффективности использованного подхода. Общая схема метода обнаружения стегоконтейнера в соответствии с предложенным методом представлена на рис. 7.

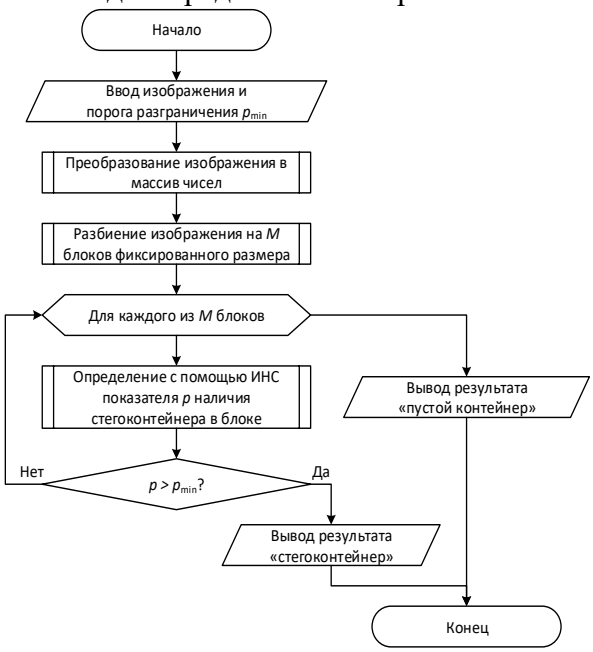

Рис.7. Общая схема метода обнаружения изображений-стегоконтейнеров с использованием разработанного метода
Fig.7. General scheme of the image-stacker detection method using the developed method

Процесс анализа блоков происходит до появления первого блока, для которого оценка принадлежности к множеству «стегоконтейнер», выработанная с помощью ИНС, окажется выше установленного порога p_{min}. Такой подход позволяет сократить время стеганодетектирования, если аналитику не требуется информация о каждом блоке для дополнительной ручной

проверки либо сбора статистики.

Таким образом, предложенный метод стеганодетектирования, основанный на применении ИНС, позволил повысить точность обнаружения изображений-стегоконтейнеров на 3,8 %, а также использовать алгоритм для изображений, имеющих большее разрешение, чем размерность входа ИНС. Результат достигнут за счёт оптимизации архитектуры ИНС и параметров обучения, а также разбиения входного изображения на блоки.

Для реализации программного модуля, осуществляющего стеганодетектирование изображений с помощью предложенного алгоритма, использована среда разработки Microsoft Visual Studio 2019, язык программирования C#. Графический интерфейс разработанного модуля представлен на рис. 8.

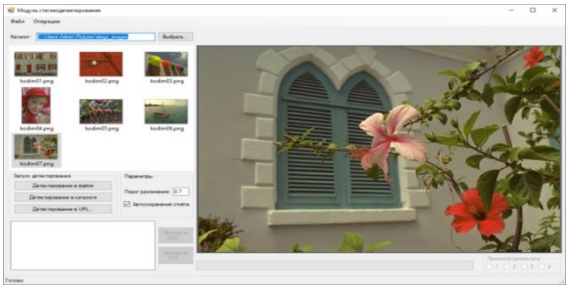

Рис.8. Пользовательский интерфейс разработанного программного модуля
Fig.8. User interface of the developed program module

К функциональным возможностям модуля относятся:

– стеганодетектирование изображений, загруженных из файла;
– стеганодетектирование изображений в выбранном каталоге;
– выгрузка изображений с веб-страниц с последующим проведением стеганодетектирования;
– формирование и вывод сведений об отдельных блоках изображения (рис. 9);
– формирование отчетов в текстовом и табличном (CSV) форматах;
– регулировка порога различения стегоконтейнеров;
– поддержка изображений форматов PNG, BMP, JPEG, GIF.

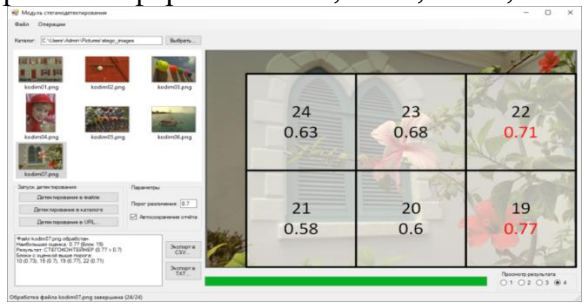

Рис.9. Просмотр результатов стеганодетектирования
Fig.9. Viewing steganodetection results

Разработанное приложение состоит из следующих модулей (рис. 10):

– модуль графического интерфейса пользователя;
– модуль загрузки изображений из файловой системы (ФС);
– модуль загрузки изображений с интернет-сайтов;
– модуль интеграции с ИНС;
– ИНС для стеганодетектирования;
– модуль формирования графических отчетов;
– модуль формирования табличных и текстовых отчетов.

Модуль графического интерфейса реализует взаимодействие с пользователем, осуществляет управление остальными модулями, а также визуализирует результаты стеганодетектирования.

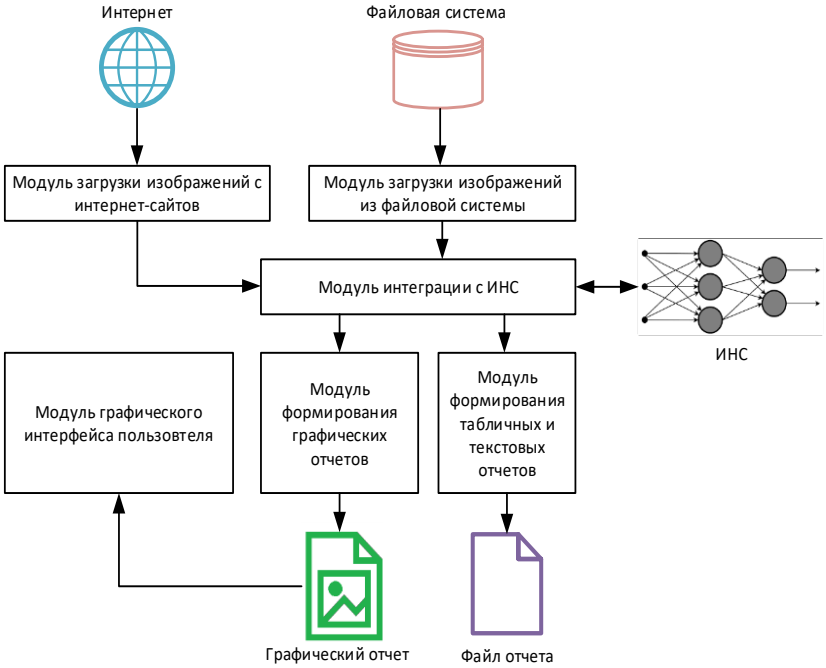

Рис.10. Схема обмена данными между модулями приложения при проведении стеганодетектирования изображений
Fig.10. Scheme of data exchange between application modules when performing image steganodetection

Модули загрузки изображений из ФС и с интернет-сайтов производят загрузку изображений в оперативную память, после чего передают их модулю интеграции с ИНС. Данный модуль выполняет преобразование фалов изображений в числовые массивы, производит формирование блоков и подает их на вход ИНС, результат работы которой сохраняет в виде массива в оперативной памяти.

В зависимости от настроек приложения, массив результатов передаётся модулям формирования графических, текстовых и табличных отчетов. Использование модульной структуры позволяет упростить разработку и дальнейшую модернизацию приложения.

Вывод. Разработанный метод предназначен для проведения стеганодетектирования в двух случаях: для выявления факта незаконного использования объектов интеллектуальной собственности: для применения в компьютерной криминалистике при идентификации изображений, содержащих скрытую и запрещенную к распространению информацию.

Входными данными при программной реализации разработанного метода являются файловый каталог или URL электронного ресурса, содержащий набор изображений, в которых требуется найти следы наличия скрытой информации.

В случае 1 входными данными будут являться источники, которые используют объекты интеллектуальной собственно: товарные знаки и промышленные образцы с нарушениями прав интеллектуальной собственности. Такими источниками могут быть недобросовестные конкуренты, пытающиеся очернить репутацию бренда, производители контрафактного контента и изделий.

В случае 2 входными данными могут являться изображения, взятые из аккаунта подозреваемого в незаконной торговле наркотиками или терроризме, которых могут содержаться стеганоконтейнеры содержащие информацию о его не законной деятельности. Например, скрытые указания, координирующая преступную группировку информация, места закладок с наркотиками и подобная информация. Выходными данными является список файлов, содержащих скрытую информацию, когда нужно определить наличие подозрительных графических файлов.

Библиографический список:

1. National Natural Science Foundation of China [Электронный ресурс]. URL: http://www.nsfc.gov.cn/english/site_1/index.html (дата обращения: 19.06.2021).
2. Ministry of Science and Technology of the People's Republic of China [Электронный ресурс]. URL: http://en.most.gov.cn/ (дата обращения: 19.05.2021).
3. Chinese Academy of Sciences [Электронный ресурс]. URL: https://english.cas.cn/ (дата обращения: 19.05.2021).
4. Cheddad A. и др. Digital image steganography: Survey and analysis of current methods // Signal Processing. 2010. Т. 90, № 3. С. 727-752.
5. Li B. и др. A Survey on Image Steganography and Steganalysis // Journal of Information Hiding and Multimedia Signal Processing с. 2011. Т. 2, № 2.
6. Dalal M., Juneja M. Steganography and Steganalysis (in digital forensics): a Cybersecurity guide // Multimed. Tools Appl. Springer, 2021. Т. 80, № 4. С. 5723-5771.
7. Breaking a steganography software: Camouflage [Электронный ресурс]. URL: http://www.guillermito2.net/stegano/camouflage/index.html (дата обращения: 20.05.2021).
8. Breaking a steganography software: JpegX [Electronic resource]. URL: http://www.guillermito2.net/stegano/jpegx/index.html (дата обращения: 20.05.2021).
9. Analyzing steganography softwares [Электронный ресурс]. URL: http://www.guillermito2.net/stegano/ (дата обращения: 20.05.2021).
10. Fridrich J., Goljan M. Practical steganalysis of digital images: state of the art // Security and Watermarking of Multimedia Contents IV. SPIE, 2002. Т. 4675. С. 1-13.
11. Kodovský J., Fridrich J. JPEG-compatibility steganalysis using block-histogram of recompression artifacts // Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics). Springer, Berlin, Heidelberg, 2013. Т. 7692 LNCS. С. 78-93.
12. Chandramouli R., Kharrazi M., Memon N. Image steganography and steganalysis: Concepts and practice // Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics). Springer Verlag, 2004. Т. 2939. С. 35-49.
13. Fridrich J., Du R., Long M. Staganalysis of LSB encoding in color images // IEEE International Conference on Multi-Media and Expo. 2000. № III/WEDNESDAY. С. 1279-1282.
14. Fridrich J., Goljan M., Du R. Reliable detection of LSB steganography in color and grayscale images // Proceedings of the ACM International Multimedia Conference and Exhibition. Association for Computing Machinery (ACM), 2001. №II. С. 27-30.
15. Lerch-Hostalot D., Megías D. Unsupervised steganalysis based on artificial training sets // Eng. Appl. Artif. Intell. Elsevier Ltd, 2016. Т. 50. С. 45-59.
16. Shi Y.Q., Chen C., Chen W. A Markov process based approach to effective attacking JPEG steganography // Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics). Springer Verlag, 2007. Т. 4437 LNCS. С. 249-264.
17. Westfeld A. Generic adoption of spatial steganalysis to transformed domain // Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics). Springer Verlag, 2008. Т. 5284 LNCS. С. 161-177.
18. Holub V., Fridrich J. Low Complexity Features for JPEG Steganalysis Using Undecimated DCT. 2014.
19. Farid H. Detecting hidden messages using higher-order statistical models // IEEE International Conference on Image Processing. 2002. Т. 2.
20. Lyu S., Farid H. Detecting hidden messages using higher-order statistics and support vectorachines // Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics). Springer Verlag, 2003. Т. 2578. С. 340-354.
21. Cohen A.S. The gaussian watermarking game / A.S. Cohen, A. Lapidoth // IEEE Transactions on Information Theory. 2002. Vol. 48(6). P. 1639-1667.

References:

1. National Natural Science Foundation of China [Electronic resource]. URL: http://www.nsfc.gov.cn/english/site_1/index.html (date of the application: 19.06.2021).
2. Ministry of Science and Technology of the People's Republic of China [Electronic resource]. URL: http://en.most.gov.cn/ (date of the application: 19.05.2021).
3. Chinese Academy of Sciences [Electronic resource]. URL: https://english.cas.cn/ (date of the application: 19.05.2021).
4. Cheddad A. и др. Digital image steganography: Survey and analysis of current methods. *Signal Processing*. 2010; 90(3):727-752.
5. Li B. and etc. A Survey on Image Steganography and Steganalysis. *Journal of Information Hiding and Multimedia Signal Processing* 2011; 2(2):15-30
6. Dalal M., Juneja M. Steganography and Steganalysis (in digital forensics): a Cybersecurity guide. *Multimed. Tools Appl. Springer*, 2021;80(4):5723-5771.
7. Breaking a steganography software: Camouflage [Electronic resource]. URL: http://www.guillermito2.net/stegano/camouflage/index.html (дата обращения: 20.05.2021).
8. Breaking a steganography software: JpegX [Electronic resource]. URL: http://www.guillermito2.net/stegano/jpegx/index.html (дата обращения: 20.05.2021).
9. Analyzing steganography softwares [Electronic resource]. URL: http://www.guillermito2.net/stegano/ (date of the application 20.05.2021).
10. Fridrich J., Goljan M. Practical steganalysis of digital images: state of the art. *Security and Watermarking of Multimedia Contents IV. SPIE*, 2002; 4675: 1-13.
11. Kodovský J., Fridrich J. JPEG-compatibility steganalysis using block-histogram of recompression artifacts . Lecture Notes in

Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics). *Springer, Berlin, Heidelberg*, 2013; 7692 LNCS: 78-93.
12. Chandramouli R., Kharrazi M., Memon N. Image steganography and steganalysis: Concepts and practice. Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics). *Springer Verlag*, 2004; 2939:. 35-49.
13. Fridrich J., Du R., Long M. Staganalysis of LSB encoding in color images. IEEE International Conference on Multi-Media and Expo. 2000;. III/WEDNESDAY:1279-1282.
14. Fridrich J., Goljan M., Du R. Reliable detection of LSB steganography in color and grayscale images. Proceedings of the ACM International Multimedia Conference and Exhibition. Association for Computing Machinery (ACM), 2001; II: 27-30.
15. Lerch-Hostalot D., Megías D. Unsupervised steganalysis based on artificial training sets. *Eng. Appl. Artif. Intell. Elsevier Ltd*, 2016; 50: 45-59.
16. Shi Y.Q., Chen C., Chen W. A Markov process based approach to effective attacking JPEG steganography. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics). Springer Verlag, 2007; 4437 LNCS: 249-264.
17. Westfeld A. Generic adoption of spatial steganalysis to transformed domain .Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics). *Springer Verlag*, 2008; 5284 LNCS: 161-177.
18. Holub V., Fridrich J. Low Complexity Features for JPEG Steganalysis Using Undecimated DCT. 2014.
19. Farid H. Detecting hidden messages using higher-order statistical models. IEEE International Conference on Image Processing. 2002; 2.
20. Lyu S., Farid H. Detecting hidden messages using higher-order statistics and support vectorachines. Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics). *Springer Verlag*, 2003; 2578: 340-354.
21. Cohen A.S. The gaussian watermarking game / A.S. Cohen, A. Lapidoth // IEEE Transactions on Information Theory. 2002; 48(6): 1639-1667.

Сведения об авторах:
Тебуева Фариза Биляловна, доктор физико-математических наук, доцент, заведующая кафедрой компьютерной безопасности; ftebueva@ncfu.ru
Огур Максим Геннадьевич, старший преподаватель кафедры компьютерной безопасности, mogur@ncfu.ru
Мандрица Игорь Владимирович, доктор экономических наук, доцент, профессор кафедры информационной безопасности; imandritsa@ncfu.ru
Чернышев Александр Борисович, доктор технических наук, профессор, профессор кафедры систем управления и информационных технологий; achernyshev@ncfu.ru
Линец Геннадий Иванович, доктор технических наук, доцент, заведующий кафедрой инфокоммуникаций; glinetc@ncfu.ru
Мочалов Валерий Петрович., доктор технических наук, профессор, профессор кафедры инфокоммуникаций; vmochalov@ncfu.ru
Information about authors:
Fariza B. Tebueva, Dr. Sci. (Eng), Assoc. Prof., Head of Computer Security Department; ftebueva@ncfu.ru
Maxim G. Ogur, Senior Lecturer, Computer Security department; mogur@ncfu.ru
Igor V. Mandritsa, Dr. Sci. (Eng), Assoc. Prof., Professor of Department of Information Security; imandritsa@ncfu.ru
Alexander B. Chernyshev, Dr. Sci. (Eng), Prof., Professor of Department of Management Systems and Information Technology; achernyshev@ncfu.ru
Gennady I. Linets, Dr. Sci. (Eng), Assoc. Prof., Head of Infocommunications Department; glinetc@ncfu.ru
Valery P. Mochalov, Dr. Sci. (Eng), Prof., Professor of Infocommunications Department; vmochalov@ncfu.ru
Конфликт интересов/Conflict of interest.
Авторы заявляют об отсутствии конфликта интересов/The authors declare no conflict of interest.
Поступила в редакцию/ Received 15.09.2022.
Одобрена после рецензирования / Reviced 12.10.2022.
Принята в печать /Accepted for publication 12.10.2022.