УДК 004.8

ОПРЕДЕЛЕНИЕ УСТОЙЧИВОСТИ БЕСКОНТЕЙНЕРНОГО МЕТОДА СОКРЫТИЯ ДАННЫХ К СОВРЕМЕННЫМ МЕТОДАМ СТЕГОАНАЛИЗА

И. В. Рудаков, к.т.н., заведующий кафедрой ИУ7 МГТУ им. Баумана, Москва, Россия;
e-mail: irudakov@bmstu.ru
М. В. Филиппов, к.т.н., доцент кафедры ИУ7 МГТУ им. Баумана, Москва, Россия;
e-mail: filippovmv@bmstu.ru
М. А. Кудрявцев, аспирант кафедры ИУ7 МГТУ им. Баумана, Москва, Россия;
orcid.org/0000-0001-7034-8270, e-mail: kudryavtsev@bmstu.ru
Д. Ю. Пудов, магистрант кафедры ИУ7 МГТУ им. Баумана, Москва, Россия;
orcid.org/0000-0003-0980-1317, e-mail: pudovdyu@mail.ru

Рассматривается задача определения возможности обнаружения скрываемых данных при помощи, разработанного авторами стеганографического метода. ***Целью работы*** *является обзор актуальных методов и инструментов поиска стегосообщений в изображениях, их применения для оценки надёжности разрабатываемого авторами метода – определения возможности обнаружения факта передачи скрываемой информации и возможности извлечения скрытых данных. В статье рассмотрены метолы стегоанализа для алгоритмов на основе статистик первого порядка, позволяющие эффективно обнаруживать искажения вследствие встраивания данных в пространственную область. Рассмотрены методы на основе различия статистик, позволяющие обнаруживать изменения в частотной области, а также методы на основе слепых классификаторов, способных обнаруживать факт сокрытия данных для большинства известных стегометодов, а также определять длины скрываемых сообщений. Рассмотрены и применены методы оценки натуральности изображений. Определяется степень устойчивости предложенного стеганографического метода к рассмотренным средствам обнаружения, приводятся рекомендации для дальнейшего улучшения метода.*

Ключевые слова: *стеганография, стеганоконтейнер, статистики первого порядка, слепые классификаторы, нейронные сети, стегоанализ, стегосообщение, сокрытие данных.*

DOI: 10.21667/1995-4565-2023-83-102-111

Введение

Стеганография – область научного знания, которая ставит своей целью сокрытие самого факта передачи информации между собеседниками. В качестве компонента для встраивания скрываемых сообщений используются так называемые стегоконтейнеры – визуально неприметные объекты-обложки (cover objects).

В общем случае стегосистемы можно представить в виде набора инструментов, реализующих механизмы встраивания и извлечения сообщений. Большинство систем при встраивании сообщений в цифровые изображения, производят незаметные человеческому глазу преобразования, получая стеганографические изображения.

С появлением методов, направленных на сокрытие факта передачи информации, появилась и получила широкое распространение область научного знания, направленная на обнаружение факта сокрытия данных, названная стеганоанализом. Её методы призваны обнаружить факт передачи скрытой информации и определить закон, по которому эти данные скрыты, тем самым, получить скрытое сообщение.

Наравне с криптоанализом, стеганографический метод считается безопасным, если в стегоизображениях не могут быть обнаружены артефакты, появившиеся вследствие встраивания. Таким образом, стегосистема считается надёжной, если не существует алгоритмов, спо-

собных определить факт наличия скрытого сообщения с вероятностью большей, чем случайное предположение.

В статье [1] предлагается разделение современных методов стегоанализа на следующие группы:

– методы на основе статистик первого порядка;

– методы на основе различия статистик высоких порядков;

– методы на основе «слепых» классификаторов.

Основным недостатком такой классификации является её ориентированность на классические стегосистемы с использованием изображений-обложек в качестве контейнеров для встраивания данных.

Современные стегосистемы в общем случае могут быть разделены на две группы – контейнерные и бесконтейнерные [2].

Контейнерные методы предполагают наличие среды (изображения, аудиосигналы, видеопоток), в который происходит встраивание сообщения. Существенным недостатком систем, основанных на встраивании информации в готовые обложки, является наличие оригинала, при определении которого можно гарантированно утверждать о факте встраивания данных. Кроме того, даже не имея оригинала, современные методы стегоанализа позволяют с высокой точностью определить алгоритм встраивания данных.

Бесконтейнерные методы характеризуются отсутствием среды для встраивания сообщений, что даёт им преимущества по сравнению с контейнерными. Бесконтейнерные методы нивелируют возможность использования классических методов стегоанализа, основанных на анализе контейнеров, к которым, в частности относятся методы, основанные на статистиках первого и более высоких порядков. Бесконтейнерные методы были описаны в ряде научных работ [3-6]. Например, в работе [6] рассматривается несколько способов генерации изображений на основе скрываемых данных без использования обложек. В рассмотренных работах основными недостатками бесконтейнерных методов считаются: маленькие размеры изображений, ограниченность скрываемых данных (отдельно рассматриваются методы сокрытия изображений, отдельно методы сокрытия текста).

Предложенный авторами метод относится к группе бесконтейнерных методов.

Целью настоящей работы является построение системы, нивелирующей описанные выше недостатки бесконтейнерных методов.

В рамках статьи применены метод «слепых» классификаторов и метод оценки натуральности изображения, для определения устойчивости разработанной стегосистемы.

Теоретическая часть

Описание предложенного метода

Предложенный авторами метод избавляет от необходимости использования контейнеров-обложек для встраивания данных. Схожий по концепции алгоритм был предложен в статье [7], однако он был ориентирован на китайский язык и использовал словари для подготовки генерируемых изображений, а также использовал облегчённую версию генеративно-состязательной сети.

Предлагаемая авторами стегосистема состоит из кодировщика и декодировщика. Схема работы кодировщика представлена на рисунке 1, декодировщик работает схожим образом, но использует инвертированный вход нейронной сети. Сгенерированные изображения стилистически схожи с набором данных, на котором происходило обучение нейронной сети и не связано с семантикой скрываемого сообщения.

Метод способен генерировать изображения с максимальным разрешением в 256x256 пикселей. Обеспечиваемый при таком размере максимально возможный объём скрываемой информации равен 36 864 байта.

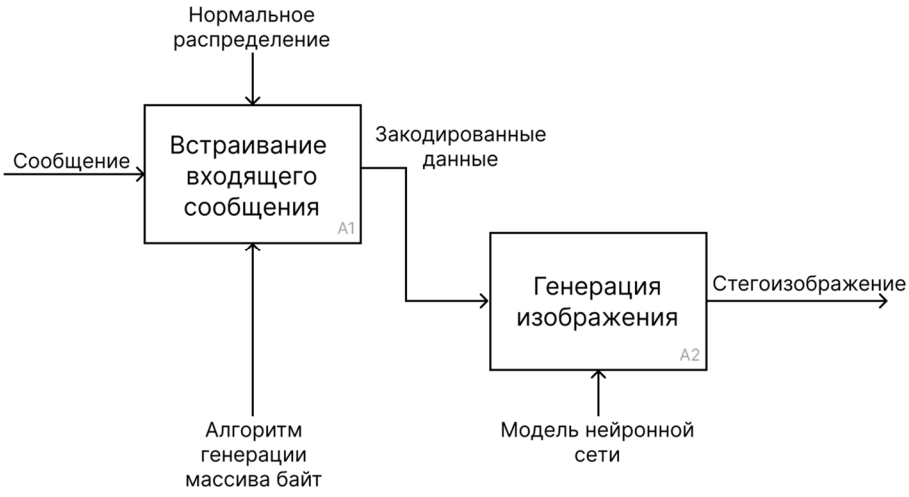

Рисунок 1 – Диаграмма работы кодировщика
Figure 1 – Encoder operation diagram

Общая идея предложенного авторами метода состоит в приведении исходного сообщения к байтовой последовательности, которая подаётся на вход нейронной сети в виде матрицы значений. На выходе нейронной сети формируется матрица значений, которая преобразуется в графический формат PNG48. Приведение к байтовой последовательности позволяет избавиться от ограничений, накладываемых на формат исходных данных, а выходной формат PNG корректно отображается практически на всех современных устройствах.

Предложенный авторами метод может быть разбит на следующие этапы:

1. Защита данных от повреждений путём использования кодов восстановления (алгоритм Соломона – Рида).
2. Генерация псевдослучайной последовательности для генерации изображения.
3. Приведение сгенерированной последовательности со встроенным в неё сообщением к нормальному распределению.
4. Использование нейронной сети для генерации изображения.
5. Преобразование выходной матрицы к графическому формату.

Рассмотрим подробнее основные этапы реализации метода.

Первый этап. Применение алгоритма Соломона – Рида

На третьем и четвёртом этапах метода возможно нарушение целостности данных. Для гарантированного сохранения исходного сообщения, авторами был применён алгоритм Соломона – Рида. Особенностью его применения к предложенному методу является необходимость применения преобразований к байтовой последовательности произвольной длины. Таким образом, входная последовательность была разбита на блоки фиксированной длины и для каждого блока были определены вспомогательные символы.

Второй этап. Генерация равномерно распределённых данных

Целью этапа является получение равномерно распределенного массива вещественных значений на основе входной байтовой последовательности. Причем важным свойством оказывается влияние всей последовательности на каждое генерируемое значение. Основой данного этапа является использование модификации линейного конгруэнтного метода. В общем случае, использованная модификация позволяет генерировать случайные равномерно распределенные целые числа по некоторому модулю:

$$x_{i+1} = F_0(x_i) = (ax_i + c) \bmod m .$$

Авторами был использован вариант генерации с двумя переменными:

$$x_{i+1} = F(x_i, x_{i-1}) = (ax_{i-1} + bx_i + c) \bmod m,$$
$$z = F(x, y) = (ax + by + c) \bmod m.$$

Третий этап. Приведение исходных данных к нормальному распределению

Используемая авторами модель нейронной сети принимает на вход вектор, имеющий стандартное нормальное распределение. На втором этапе был получен вектор нужного размера, но имеющий равномерное распределение. Таким образом, на этом этапе необходимо применить обратимое преобразование.

Авторами было использовано преобразование Бокса – Мюллера в тригонометрической форме, которое из пары независимых равномерно распределенных величин в интервале (0, 1) позволяет получить пару независимых нормально распределенных величин:

$$z_0, z_1 = BM(r, a),$$
$$z_0 = \cos 2\pi a \sqrt{-2 \ln r},$$
$$z_1 = \sin 2\pi a \sqrt{-2 \ln r}.$$

Обратное преобразование выполняется следующим образом:

$$s = \sqrt{(z_0^2 + z_1^2)},$$
$$r = \exp \frac{-s^2}{2},$$
$$\sin Val = \frac{z_1}{s},$$
$$\cos Val = \frac{z_0}{s},$$
$$a = \arcsin \sin Val.$$

При реализации необходимо отслеживать корректное восстановление угла a после применения arcsin. В некоторых случаях может потребоваться изменение четверти, в которую попал угол. Это можно отследить путем анализа знаков синуса и косинуса ($\sin Val$ и $\cos Val$).

Четвёртый этап. Применение нейронной сети

Предложенный авторами метод использует в качестве генератора изображений потоковую модель нейронной сети. Структура нейронной сети, используемая в рамках предложенного метода, подробно рассмотрена в статье [8]. В рамках этапа необходимо преобразовать одномерный массив нормально распределенных вещественных чисел размера $H * W * 3$ в тензор формы [1][3][H][W], ожидаемый нейросетью.

Выходными данными нейросети является тензор аналогичного размера [1][3][H][W], причем распределение элементов этого вектора соответствует нормальному распределению. Для приведения к отрезку [0, 1] будем использовать сигмоиду:

$$y = \frac{1}{e^{\frac{-x}{k}} + 1},$$

где $k > 0$. Таким образом, «рабочая область» сигмоиды находится в диапазоне [-5, 5].

Следует отметить, что величина y при выполнении обратного преобразования может претерпеть изменения – накопить погрешность. Для компенсации возможной ошибки авторы используют принудительное ограничение диапазона величины y перед выполнением преобразования:

$$eps = 1e-5,$$
$$y' = \max(eps, \min(1-eps, y)),$$
$$x' = (\log y' - \log(1-y')) * k.$$

Коэффициент k помогает найти компромисс, так как, с одной стороны, чем меньше k, тем больший выходной диапазон сигмоиды приходится на рабочую входную область, и, следовательно, тем меньше будет погрешность в результате прямого и обратного преобразований. А с другой стороны, чем больше k, тем «толще» будут концы сигмоиды вблизи граничных значений и тем выше будет распознаваемый диапазон.

Пятый этап. Подготовка контейнера в PNG 48bit

Выходным значением нейронной сети является вектор вещественных чисел (float32) размером [3][H][W]. Значения элементов вектора гарантированно принадлежат интервалу [0, 1].

PNG файл способен хранить не более 2 байт полезной информации. Авторами был предложен способ сохранения точности сохраняемой трансформации за счет использования дополнительного байта памяти. Для каждого кодируемого числа из исходного вектора получается два целых числа – p (тип uint16, 2 байта) и q (тип uint8, 1 байт). При этом значение p остаётся в области допустимых значений выбранного формата, что обеспечивает сохранность исходного цвета изображения. На q никаких ограничений не накладывается – это значение необходимо исключительно для обеспечения возможности декодирования.

После применения рассмотренного преобразования ко всем элементам полученного на предыдущем этапе вектора, из значений p составляется uint16-массив [H][W][3], который и считается итоговым png-изображением, а из значений q формируется еще один uint16-массив размером [H/2][W][3]. Последовательные значения q попарно объединяются и образуют 2-байтные значения. В случае нечетной высоты изображения последний ряд заполняется лишь наполовину, при этом в оставшиеся позиции записываются случайные значения для увеличения надёжности алгоритма.

Последним шагом является модификация заголовка PNG файла для скрытия матрицы значений q.

Обзор методов стегоанализа

«Слепые» классификаторы

В данном разделе ограничимся рассмотрением атак, используемых для бесконтейнерных методов.

Современные стегосистемы для сокрытия информации используют механизмы встраивания в пространственную, частотную, статистическую и структурную области. Для минимизации возможности обнаружения канала скрытой передачи данных, в качестве функции распределения данных в контейнере всё чаще используются нейронные сети. В связи с этим возникла потребность в методах стегоанализа, способных определить наличие скрытого канала вне зависимости от используемого метода и выбранного изображения-обложки.

Развитие таких методов стегоанализа началось с работы Фарида [9], который предложил использовать 72 признака, вычисляемых вейвлет-преобразованием. По этим признакам при помощи метода опорных векторов проводилось разделение изображений на стеганографические и обыкновенные. В основе обучения метода опорных векторов ставились стегоизображения и их контейнеры.

Метод, предложенный Фаридом, позволяет:

– для стеганографических методов в частотной области – выявить схему встраивания данных;

– для стеганографических методов других групп – определять факт наличия сокрытой информации и оценивать длину скрытого сообщения.

В статье [10] предлагается усовершенствование «слепого классификатора» для работы с признаками, вычисляемыми при помощи коэффициентов ДКП. Выделяется 2 типа признаков: первого и второго порядков. Признаки могут быть вычислены по формуле (1):

$$f = \| F(J_1) - F(J_2) \|_{L_1} . \quad (1)$$

Норма L_1 для признака f вычисляется как сумма модулей всех элементов вектора или матрицы. Векторный функционал F применяется к изображению J_1. Изображение J_1 обрезается на 4 пикселя в каждом направлении, после чего расширяется согласно таблице квантования для J_1. Таким образом получается изображение J_2, к которому повторно применяется F.

Такие классификаторы улучшают идею стегоанализа на основе статистик высокого порядка.

Методы оценки «натуральности» изображений

Основной работой в области активного стегоанализа на основе нейронных сетей является статья Юнга и Бэ [11]. Предлагаемый в ней метод ориентирован на атаки моделей глубокого обучения, которые используют стегоконтейнер.

Основная идея состоит во введении шума в каждый пиксель на основе нейронной сети для того, чтобы сохранить стегоизображение внешне, но исключить возможность сохранения скрытого канала. Основная проблема такого метода заключается в том, чтобы узнать, какой исходный набор данных использовался для обучения и какая нейронная сеть формирует стегоизображения. Иначе получаемый шум может иметь негативное влияние на «очищенное» изображение.

Помимо прямых методов стегоанализа могут быть применены методы, предназначенные для обнаружения и анализа фейковых изображений, в особенности, лиц. Среди них можно выделить следующие:

– метод Куана на основе свёрточной нейронной сети [12];
– метод Гангана на основе модифицированной архитектуры EfficientNet [13];
– метод Жанга на основе корреляции пикселей и каналов изображений [14];
– метод Раймуни на основе свёрточной нейронной сети [15];
– метод Гунавана на основе свёрточной нейронной сети [16].

Среди перечисленных методов следует выделить метод Гунавана. Основным его преимуществом является возможность анализа признаков независимо от предметной области, в то время как методы Гангана, Жанга, Раймуни и Куана сильно завязаны на архитектурах нейронных сетей, предназначенных для распознавания лиц. В то же время метод Гунавана позволяет обучать классификатор для изображений из различных предметных областей, определяемых поставленной задачей. Метод основан на анализе уровня ошибок ELA (error level analysis). Идея анализа уровня ошибок состоит в независимом сжатии каждых участков 8x8 исходного изображения. Если изображение не содержит манипуляций, то частота ошибок будет примерно одинаковой для всего изображения.

Практическое применение рассмотренных методов стегоанализа

Применим рассмотренные методы стегоанализа к предложенному авторами методу.

Методы слепых классификаторов

Для анализа статистических, пространственных и структурных стегометодов была использована программа Aletheia [17]. При помощи «слепых» классификаторов Aletheia позволяет находить информацию, скрытую методами F5, Steghide, SteganoGAN, адаптивными схемами и разновидностями LSB.

В состав Aletheia входят классификаторы на основе архитектуры EfficientNet B0 и метода опорных векторов. Модели EfficientNet B0 были обучены на наборе данных «Alaska2», а модель на основе опорных векторов обучена на наборе данных «Bossbase».

Описанный программный комплекс был обучен на той же исходной выборке, что и метод, предложенный авторами.

В результате работы Aletheia не обнаружила аномалий, связанных с встраиванием данных.

Отметим, что предложенный авторами метод не содержит модификаций исходного контейнера, генерируя изображения на основе исходной информации, что подтверждает устойчивость предложенного метода к методам стегоанализа на основе слепых классификаторов.

Методы оценки натуральности изображений

Для обучения методом Гунавана был использован набор данных «102 Category Flower Dataset», объединенный с набором изображений, сгенерированных предложенной моделью. Изображения из «102 Category Flower Dataset» получили метку «натуральные», а сгенерированные соответственно «ложные». Выбор набора данных основан на том, что сама модель при обучении использовала такую же исходную выборку.

На рисунках 2 и 3 приводится пример различия ELA, вычисленного для стегоизображения и реальной фотографии.

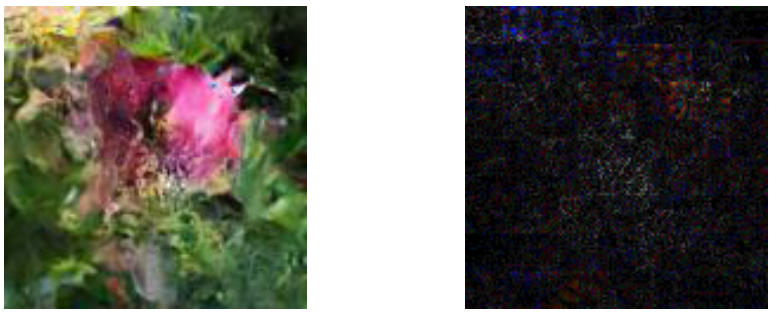

Рисунок 2 – Сгенерированное стегоизображение и его ELA маска
Figure 2 – Generated image and its ELA mask

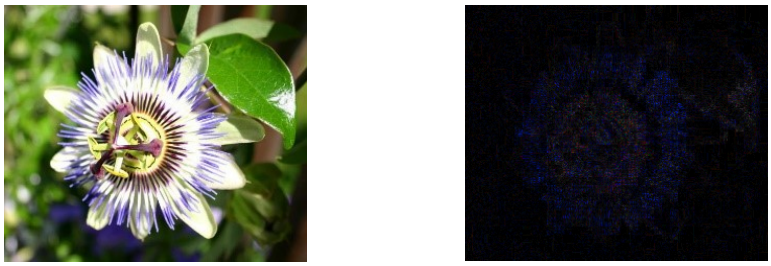

Рисунок 3 – Реальное изображение и его ELA маска
Figure 3 – Real image and its ELA mask

Метод Гунавана способен обнаружить факт генерации изображения, однако он не способен обнаружить факт применения стегометода, а кроме того, для получения качественного результата потребовалось обучить модель на той же исходной выборке, что и нейронную сеть, используемую для генерации изображения. Такой подход крайне трудно применим при анализе изображений в чужеродной среде.

Заключение

В рамках статьи кратко рассмотрена классификация современных методов стегоанализа. Наиболее известные представители каждой группы были применены к разрабатываемому методу бесконтейнерного сокрытия данных. Большинство современных методов используют математические алгоритмы или эвристики, сравнивающие оригинальное изображение с контейнером-обложкой. Ожидаемо, такие методы не смогли обнаружить факт сокрытия данных,

в связи с отсутствием контейнера. Таким образом, можно сделать вывод о том, что предложенный метод является устойчивым к большинству современных методов стегоанализа. Методы на основе слепых классификаторов ошибочно обнаружили модификации наименьших значащих бит, а метод Гунавана, обученный на той же исходной выборке что и используемая при сокрытии данных модель, выявил факт генерации изображений. Тем не менее, этот факт не даёт возможности гарантированно определить наличие скрытого канала, но он может быть потенциальным демаскирующим признаком при анализе передаваемых изображений. Кроме того, он даёт понимание причины ложного обнаружения LSBM-модификации. Таким образом, метод Гунавана может быть использован в качестве критика при генерации изображений, что позволит значительно улучшить алгоритм и является предметом дальнейших исследований.

Библиографический список

1. **Fridrich J.** Feature-Based Steganalysis for JPEG Images and its Implications for Future Design of Steganographic Schemes // In: Information Hiding / Ed. by Fridrich J. Toronto: Springer, 2004. pp. 67-81.

2. **Qin J., Luo Y., Xiang X., Tan Y., Huang H.** Coverless Image Steganography: A Survey // IEEE Access. 2019. No. 7. pp. 171372-171394.

3. **Xiyao Liu, Zhaoying Li, Junxing Ma, Wei Zhang, Jian Zhang, Yipeng Ding.** Robust coverless steganography using limited mapping images // Journal of King Saud University – Computer and Information Science. 2022. No. 34. pp 4472-4482.

4. **Qiang Liu, Xuyu Xiang, Jiaohua Qin, Yun Tan, Junshan Tan, Yuanjing Luo.** Coverless steganography based on image retrieval of DenseNet features and DWT sequence mapping // Knowledge-Based Systems. 2020. No. 192.

5. **Qi Li, Xingyuan Wang, Xiaoyu Wang, Bin Ma, Chunpeng Wang, Yunqing Shi.** An encrypted coverless information hiding method based on generative models // Information Sciences. 2021. No 553. pp. 19-30.

6. **Guofeng Li, Bingwen Feng, Mingjin He, Jian Weng, Wei Lu.** High-capacity coverless image steganographic scheme based on image synthesis // Signal Processing: Image Communication. 2023. No. 111.

7. **Liu M. M., Zhang M. Q., Liu J., Zhang Y. N., Ke Y**. Coverless Information Hiding Based on Generative adversarial networks. URL: https://arxiv.org/abs/1712.06951 (дата обращения 22.05.2022).

8. **Казаков К. Е., Кудрявцев М. А.** Mmflow: масштабируемая потоковая модель для генерации изображений // Вестник РГГУ. Серия: информатика. Информационная безопасность. Математика. 2022. С. 59-76.

9. **Farid H., Lyu S.** Detecting Hidden Messages Using Higher-Order Statistics and Support Vector Machines // Lecture Notes in Computer Science. Noordwijkerhout. 2002. Vol. 2578. pp. 340-354.

10. **Cachin C.** An Information-Theoretic Model for Steganography // Lecture Notes in Computer Science. Portland. 1998. Vol. 1525. pp. 306-318.

11. **Jung D., Bae H., Choi H. S., Yoon S.** PixelSteganalysis: Pixel-wise Hidden Information Removal with Low Visual Degradation // IEEE Transactions on Dependable and Secure Computing. 2019. pp. 1-12.

12. **Quan W., Wang K., Yan D. M., Zhang X.** Distinguishing Between Natural and Computer-Generated Images Using Convolutional Neural Networks // IEEE Transactions on Information Forensics and Security, Vol. 13, No. 11, November 2018. pp. 2772-2787.

13. **Gangan M., Anoop K., Lajish V.** Distinguishing Natural and Computer-Generated Images using Multi-Colorspace fused EfficientNet // Computer Vision and Pattern Recognition. 2021. pp. 1-13.

14. **Zhang R.S., Quan W. Z., Fan L. B., Hu L. M., Yan D. M.** Distinguishing Computer-Generated Images from Natural Images Using Channel and Pixel Correlation // Journal of Computer Science and Technology. 2020. Vol. 35, pp. 592-602.

15. **Rahmouni N., Nozick V., Yamagishi J.** Distinguishing computer graphics from natural images using convolution neural networks // 2017 IEEE Workshop on Information Forensics and Security (WIFS). Rennes. 2017. pp. 1-6.

16. **Gunawan A., Lovenia H., Pramudita A. Deteksi** Pemalsuan Gambar dengan ELA dan Deep Learning. Bandung, 2018.

17. **Lerch-Hostalot**. Aletheia. GitHub, Inc. 2021. URL: https://github.com/daniellerch/aletheia (дата обращения: 03.06.2022).

UDC 004.8

EFFICIENCY DETERMINING FOR THE CONTAINERLESS DATA HIDING METHOD AGAINST THE MODERN METHODS OF STEGANALYSIS

I. V. Rudakov, Ph.D. (Tech.), BMSTU, Moscow, Russia;
e-mail: irudakov@bmstu.ru

M. V. Filippov, Ph.D. (Tech.), BMSTU, Moscow, Russia;
e-mail: filippovmv@bmstu.ru

M. A. Kudryavtsev, post-graduate student, BMSTU, Moscow, Russia;
orcid.org/0000-0001-7034-8270, e-mail: kudryavtsev@bmstu.ru

D. Yu. Pudov, Master's student, BMSTU, Moscow, Russia;
orcid.org/0000-0003-0980-1317, e-mail: pudovdyu@mail.ru

Article consider the problem of detecting data hidden by the steganographic method developed by the authors. ***The aim of the article is*** *to review the current methods and tools destined for discovering hidden messages in images, their applicability to assess the reliability of the method developed by the authors. Determine the possibility of detecting the transmission of hidden information and the possibility of extracting hidden data. The article discusses steganalysis methods for algorithms based on first-order statistics, which effectively detect distortions due to data embedding in a spatial domain. Authors conside the methods based on differences in statistics, which allow to detect changes in the frequency domain, as well as methods based on blind classifiers that can detect the fact of hiding data by most known steganographic methods, as well as determine the lengths of hidden data. Finally authors consider methods for assessing the naturalness of images and applying all discussed steganalysis methods for proposed method. At the end authors give recommendations for the further improvement of thir method.*

Keywords: *steganography, container, first-order statistics, blind classifiers, neural networks, stegoanalysis, secret message, data hiding.*

DOI: 10.21667/1995-4565-2023-83-102-111

References

1. **Fridrich J.** Feature-Based Steganalysis for JPEG Images and its Implications for Future Design of Steganographic Schemes. *In: Information Hiding* / Ed. by Fridrich J. Toronto: Springer, 2004. pp. 67-81.

2. **Qin J., Luo Y., Xiang X., Tan Y., Huang H.** Coverless Image Steganography: A Survey. *IEEE Access*. 2019, no. 7, pp. 171372-171394.

3. **Xiyao Liu, Zhaoying Li, Junxing Ma, Wei Zhang, Jian Zhang, Yipeng Ding.** Robust coverless steganography using limited mapping images. *Journal of King Saud University – Computer and Information Science*. 2022, no. 34, pp 4472-4482.

4. **Qiang Liu, Xuyu Xiang, Jiaohua Qin, Yun Tan, Junshan Tan, Yuanjing Luo.** Coverless steganography based on image retrieval of DenseNet features and DWT sequence mapping. *Knowledge-Based Systems*. 2020, no. 192.

5. **Qi Li, Xingyuan Wang, Xiaoyu Wang, Bin Ma, Chunpeng Wang, Yunqing Shi.** An encrypted coverless information hiding method based on generative models. *Information Sciences*. 2021, no 553, pp. 19-30.

6. **Guofeng Li, Bingwen Feng, Mingjin He, Jian Weng, Wei Lu.** High-capacity coverless image steganographic scheme based on image synthesis. *Signal Processing: Image Communication*. 2023, no. 111.

7. **Liu M.M., Zhang M.Q., Liu J., Zhang Y.N., Ke Y**. Coverless Information Hiding Based on Generative adversarial networks. URL: https://arxiv.org/abs/1712.06951 (accessed: 22.05.2022).

8. **Kazakov K. E., Kudryavtsev M. A.** Mmflow: masshtabiruemaya potokovaya model' dlya generacii izobrazhenij. *Vestnik RGGU. Seriya: informatika. Informacionnaya bezopasnost'. Matematika*. 2022, pp. 59-76. (in Russian).

9. **Farid H., Lyu S.** Detecting Hidden Messages Using Higher-Order Statistics and Support Vector Machines. *Lecture Notes in Computer Science. Noordwijkerhout*. 2002, vol. 2578, pp. 340-354.

10.**Cachin C.** An Information-Theoretic Model for Steganography. *Lecture Notes in Computer Science*. Portland. 1998, vol. 1525, pp. 306-318.

11.**Jung D., Bae H., Choi H.S., Yoon S.** PixelSteganalysis: Pixel-wise Hidden Information Removal with Low Visual Degradation. *IEEE Transactions on Dependable and Secure Computing*. 2019, pp. 1-12.

12.**Quan W., Wang K., Yan D. M., Zhang X.** Distinguishing Between Natural and Computer-Generated Images Using Convolutional Neural Networks. *IEEE Transactions on Information Forensics and Security*. November 2018, vol. 13, no. 11,. pp. 2772-2787.

13.**Gangan M., Anoop K., Lajish V.** Distinguishing Natural and Computer-Generated Images using Multi-Colorspace fused EfficientNet. *Computer Vision and Pattern Recognition*. 2021. pp. 1-13.

14.**Zhang R. S., Quan W. Z., Fan L. B., Hu L. M., Yan D. M.** Distinguishing Computer-Generated Images from Natural Images Using Channel and Pixel Correlation. *Journal of Computer Science and Technology*. 2020, vol. 35, pp. 592-602.

15.**Rahmouni N., Nozick V., Yamagishi J.** Distinguishing computer graphics from natural images using convolution neural networks. *2017 IEEE Workshop on Information Forensics and Security (WIFS). Rennes*. 2017. pp. 1-6.

16.**Gunawan A., Lovenia H., Pramudita A. Deteksi** *Pemalsuan Gambar dengan ELA dan Deep Learning*. Bandung, 2018.

17.**Lerch-Hostalot**. Aletheia. GitHub, Inc. 2021. URL: https://github.com/daniellerch/aletheia (accessed: 03.06.2022).