УДК 004.8 DOI: 10.18698/0236-3933-2023-1-83-97

МЕТОД ГЕНЕРАЦИИ ИЗОБРАЖЕНИЙ С ИСПОЛЬЗОВАНИЕМ НЕЙРОННЫХ СЕТЕЙ НА ОСНОВЕ ВОССТАНАВЛИВАЕМОЙ БАЙТОВОЙ ПОСЛЕДОВАТЕЛЬНОСТИ

И.В. Рудаков irudakov@bmstu.ru
М.В. Филиппов filippovmv@bmstu.ru
М.А. Кудрявцев kudryavtsev@bmstu.ru

МГТУ им. Н.Э. Баумана, Москва, Российская Федерация

Аннотация

В связи со стремительным развитием информационных технологий задачи обеспечения целостности, сохранности и конфиденциальности информации, а также возможность гарантированного подтверждения ее источника становятся актуальны как никогда. Одним из возможных решений этой задачи могут быть стеганографические методы, позволяющие как скрывать факт передачи информации, так и незаметно добавлять полезные данные. В научной литературе описано большое число стеганографических алгоритмов. Однако лишь незначительное число работ посвящено методам сокрытия данных с использованием нейронных сетей и еще меньше генерации контейнеров для них. Предложен метод генерации изображений на основе скрываемой информации, гарантирующий возможность как сокрытия, так и последующего извлечения информации, исключая необходимость выбора подходящего контейнера. В рамках метода разработан алгоритм, включающий в себя описание этапов предобработки входных данных, преобразования в изображение-контейнер и извлечения скрытой информации. Приведены примеры работы предложенного метода. Метод может служить как в качестве стеганографического алгоритма сокрытия информации, так и алгоритма добавления информации в виде водяных знаков

Ключевые слова

Стеганография, сокрытие информации, водяные знаки, генерация изображений, нейронные сети

Поступила 05.04.2022
Принята 08.11.2022

Введение. Обеспечение целостности, сохранности и конфиденциальности передаваемой информации — одна из старейших задач, стоящих перед человеком. Для ее решения используются как криптографические средства, делающие информационные сообщения недоступными к прочтению без специальных ключей, так и стеганографические — скрывающие факт

передачи ценной информации. Как правило, криптография работает с текстовым представлением информации, а стеганография ставит целью встраивания одной части информации в другую — будь то текст, изображение или аудиосигнал. Данные, в которые встраивается ценная информация, называются контейнерами, ценная информация — сообщением.

В современном мире классические контейнеры получили цифровое представление, создав в том числе более сложные — составные контейнеры (видеопоследовательности — совокупность набора изображений с возможным добавлением аудиосигнала) [1].

Здесь рассмотрены алгоритмы сокрытия данных в изображениях. Несмотря на множество характеристик, большинство стеганографических методов, скрывающих информацию в изображениях, хорошо изучено и не обеспечивает достаточной защищенности скрываемых данных [2]. В связи с этим необходимо разработать новый метод сокрытия информации, устойчивый к современным методам стеганоанализа.

Обзор существующих методов. Перечислим классические стеганографические методы.

Сокрытие информации в пространственной области. Основное преимущество — отсутствие необходимости выполнения вычислительно-сложных или долгих математических преобразований. К недостаткам можно отнести крайне низкую устойчивость к искажениям, в частности компрессиям, а также относительную простоту обнаружения факта разрушения существующих зависимостей между битами с использованием теории вероятности и математической статистики [3].

Метод замены наименее значащего бита — наиболее распространенный метод замены в пространственной области [4]. Наименьший значащий бит изображения хранит минимальный объем полезной информации, в большинстве случаев человеческий глаз не способен заметить его модификации. Объем встраиваемых данных может занимать до 1/8 общего объема контейнера. В предельных случаях возможна замена двух последних бит, что может увеличить объем хранимой информации в 2 раза [5].

Сокрытие информации в частотной области. Для представления изображения в частотной области применяется декомпозиция изображения-контейнера. Существуют методы на основе дискретного косинусного преобразования (ДКП), дискретного преобразования Фурье, вейвлет-преобразований. Преобразования могут применяться ко всему изображению и к отдельным его частям. Методы получили наибольшее распространение вследствие их использования в сжатии JPEG-изображений [6], что гарантирует большую устойчивость полезной информации к сжатию.

Метод относительной замены коэффициентов ДКП — один из наиболее распространенных методов сокрытия информации [7]. Идея метода заключается в разбиении изображения на блоки размером 8 × 8 пикселей. Дискретные косинусные преобразования применяются к каждому блоку. В результате получаются матрицы коэффициентов ДКП размером 8 × 8, в которые можно сохранить 1 бит полезной информации. Коэффициенты могут выбираться псевдослучайно.

Статистические методы. Основаны на определенных статистических свойствах изображения. Идея заключается в частичном или полном изменении некоторых статистических характеристик изображения-контейнера, при которых принимающая сторона сможет определить наличие скрытого сообщения.

Основная сложность, ограничивающая применимость таких методов, — необходимость определения полной информации о статистической метрике для изображения-контейнера как у отправляющей, так и у принимающей стороны. В результате имеет место высокая сложность описания функции обнаружения скрытой информации $f(b_i)$, где f — тестовая функция; b_i — проверяемый блок изображения.

Структурные методы. Основаны на методах сокрытия информации в пространственной и частотной областях. Пример реализации — алгоритм, предложенный в [8]. Идея заключается в использовании семаграмм — сообщений, в которых шифрообозначениями могут быть любые символы, кроме букв и цифр. Сокрытие информации проводится на содержательном уровне с применением структурных и информационных параметров изображения-контейнера. Например, если на изображении присутствуют точки и тире, то часть изображения может быть модифицирована для передачи сообщения с помощью азбуки Морзе.

Перечисленные методы являются базовыми и демонстрируют преимущества и недостатки каждого подхода. Актуальные методы каждой группы описаны в [9–11]. Пропускная способность большинства методов находится в обратной зависимости от качества изображения, а скрываемая информация может быть обнаружена при активном или пассивном стеганографическом анализе.

Методы с применением нейронных сетей. В этих методах используются наработки в области нейронных сетей для автоматизированного выбора частей изображения в целях встраивания исходного сообщения. Такой подход делает невозможным применение классических методов стеганографического анализа.

Впервые эта идея реализована и описана в [12]. Основные недостатки — ограничения, накладываемые на размер изображения (32×32 пикселя) и скрываемое сообщение. Алгоритм умел скрывать только изображения внутри других изображений, также не был определен предельный размер возможного скрываемого сообщения.

Для исключения описанных недостатков разработан и реализован метод, получивший название SteganoGAN [13] и состоящий из кодировщика, декодировщика и критика.

На вход кодировщика подается изображение-контейнер (C) с полезной информацией в виде битового вектора $M \in \{0,1\}^{D \times W \times H}$, где D — номер бита в пикселе; W — ширина; H — высота [1, 6], в результате возвращается изображение со спрятанным сообщением $S = \varepsilon(C, M)$, ε — функция кодировщика.

Декодировщик принимает на вход изображение с вшитым сообщением $D(S)$ и возвращает исходное сообщение M.

Для оптимизации работы алгоритмов кодировщика и декодировщика необходим критик. Он представляет собой нейронную сеть, входящую в GAN и необходим для минимизации вероятности получения ошибки при работе декодера, а также для поиска минимального расстояния от изображения-контейнера до оригинального изображения. Критик отвечает за максимизацию внешней схожести между изображением-контейнером и оригинальным изображением.

Метод SteganoGAN сильно зависит от исходной обучающей выборки, поскольку функция распределения ориентирована на определенный набор характеристик, формируемых нейронной сетью. Существенным недостатком является отсутствие валидации при работе кодировщика — алгоритм не проверяет успешность операции встраивания сообщения.

Преимущества и недостатки каждой группы методов приведены в таблице.

Следовательно, большинство современных стеганографических алгоритмов ориентированы на поиск решения проблем классических методов путем добавления более сложных механизмов сокрытия сообщений с сохранением основных понятий — контейнера, исходного и скрываемого сообщений. Кроме того, с развитием информационных систем увеличилось число способов анализа и обнаружения факта модификации изображений, что еще сильнее снизило эффективность существующих методов.

Сравнение стеганографических методов

Метод	Возможность обнаружения	Подверженность стеганографическому анализу	Устойчивость к сжатию
Сокрытие информации в области: пространственной	Высокая		Низкая
частотной	Средняя	Высокая	Средняя
Статистические	Низкая		
Структурные	Средняя	Низкая	Средняя
С применением нейронных сетей	Средняя	–	Низкая

Метод генерации контейнеров. Современные нейронные сети позволяют стилизовать и генерировать новые уникальные изображения, похожие на обучающий набор данных.

Предлагаемый метод позволяет отказаться от контейнеров ввиду генерации оригинальных изображений на основе байтового представления информационных сообщений. Поскольку на вход принимается байтовая последовательность, метод одинаково эффективно скрывает информацию любого типа, а именно текст, изображение, аудиосигнал.

Сгенерированные изображения стилистически схожи с набором данных, на котором происходило обучение нейронной сети, и не связано с семантикой скрываемого сообщения. Предлагаемый метод (рис. 1) содержит четыре этапа.

1. Обработка скрываемых данных.
2. Генерация изображения.
3. Обработка изображения.
4. Декодирование изображения.

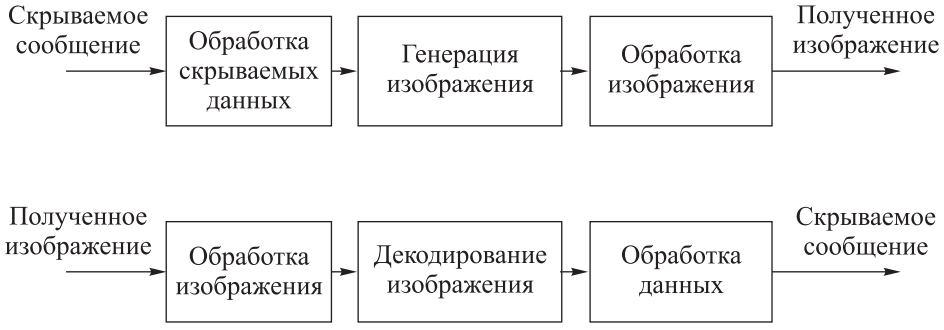


Рис. 1. Общая схема работы предлагаемого алгоритма

Обработка скрываемых данных. Обученная модель нейронной сети принимает на вход изображение размером 64 × 64 пикселя. Потенциальная пропускная способность может быть вычислена по формуле $M = Ш \cdot К \cdot В$, где *Ш*, *В*, *К* — ширина, высота и число каналов изображения, при этом *В* представляет собой размер элемента входной матрицы (4 байта для вещественных чисел типа *float*). Таким образом, потенциальная пропускная способность для изображения размером 64 × 64 пикселя составит $M = 64 \cdot 64 \cdot 3 \cdot 4 = 49152$ байта. Исходя из особенностей архитектуры используемой нейронной сети, реальный размер скрываемого сообщения должен быть не более 75 % потенциальной пропускной способности. С учетом ограничения максимальный размер скрываемого сообщения *S* не должен превышать 36 864 байта.

В зависимости от размера скрываемого сообщения может использоваться один из подходов к обработке входящей информации *I*.

1. Размер скрываемого сообщения превышает половину максимального размера сообщения (рис. 2). В этом случае предлагается применить функцию *transform(I)*, которая уменьшит число повторяющихся символов. В качестве такой функции может использоваться хэширование или криптографический алгоритм. Тогда ключ становится частью скрываемого сообщения, что необходимо учитывать при скрытии.

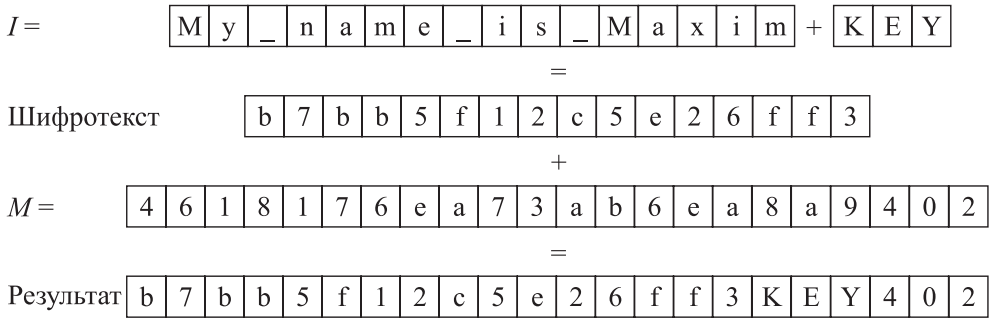


Рис. 2. Кодирование данных, превышающих половину максимального размера сообщения

2. Размер скрываемого сообщения меньше половины максимального размера сообщения (рис. 3). В этом случае предлагается применить функцию *shuffle(I)*, которая каждый байт скрываемого сообщения будет подставлять в сгенерированный массив с шагом $step = M / (SP)$, где P — число повторений скрываемого сообщения в массиве байт, диапазон $[1, round(M / P)]$.

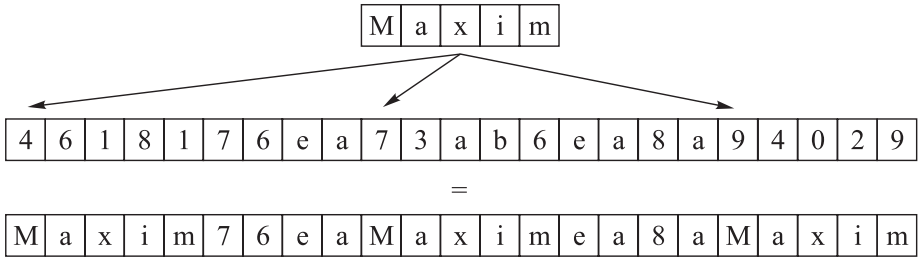


Рис. 3. Кодирование данных, размер которых меньше половины размера максимального сообщения

После формирования байтового представления скрываемого сообщения к полученному массиву применяется линейное нормирование в диапазоне (–1, 1). Исходя из особенностей предметной области, полученные данные подчиняются стандартному нормальному распределению.

Декодирование функционально аналогично кодированию — первым этапом осуществляется линейное нормирование, затем полученная матрица поступает в инвертированный вход и на выходе преобразуется обратно в байтовую последовательность.

Генерация и декодирование изображения. Для реализации метода обучена модель, основанная на архитектуре Real NVP [14] и ориентированная на стилизацию изображений. Общий вид архитектуры нейронной сети показан на рис. 4.

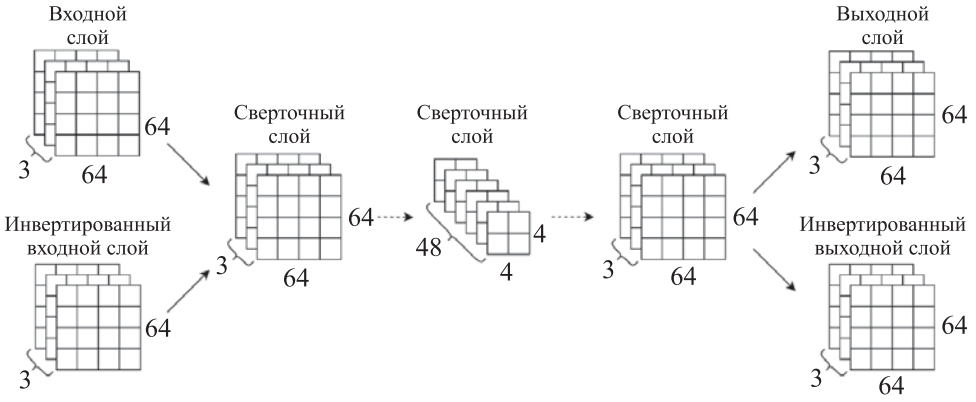


Рис. 4. Общий вид архитектуры нейронной сети

Рассматриваемая модель имеет два входных и два выходных слоя. Одна пара необходима для генерации изображения из информационного сообщения, вторая — для получения исходного сообщения из изображения. Каждый вход принимает изображение в виде матрицы вещественных чисел со стандартным нормальным распределением.

Нейронная сеть содержит набор парных связующих слоев (Coupling layers) [15], состоящих из преобразований по маскам *checkerboard* и *channel-wise*.

Схема свертки (рис. 5) включает в себя четыре связующих слоя, содержащих шесть преобразований (три *checkerboard* и три *channel-wise*), и один слой, состоящий из четырех преобразований *checkerboard*.

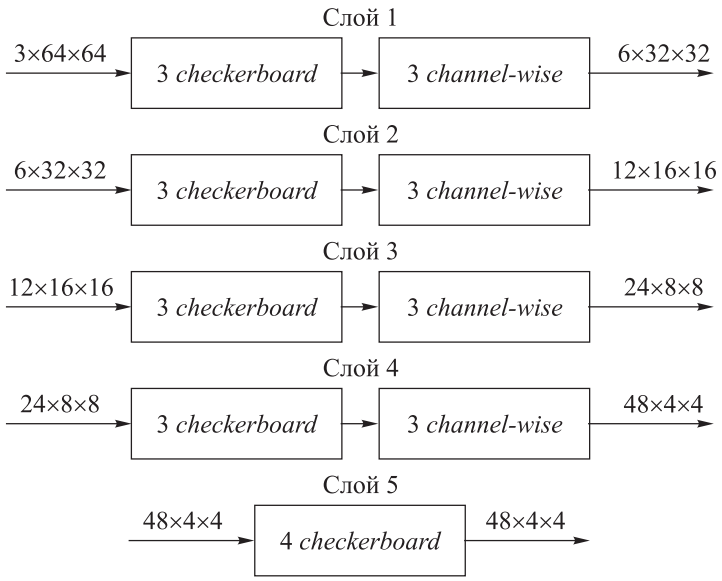


Рис. 5. Схема свертки

Слои обратного преобразования также включают в себя операцию *squeeze* — снижения размерности входного тензора. Тензор размером 4 × 4 × 1 представлен на рис. 6, *а*, преобразованный тензор размером 2 × 2 × 4 — на рис. 6, *б*.

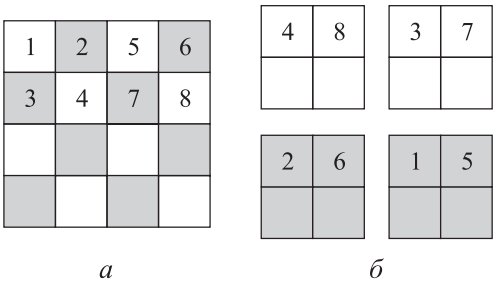


Рис. 6. Операция squeeze

Операция повышения расширения похожа на процесс свертки, но в начале и конце каждого слоя добавляются операции *squeeze*, *undo_squeeze* (рис. 7).

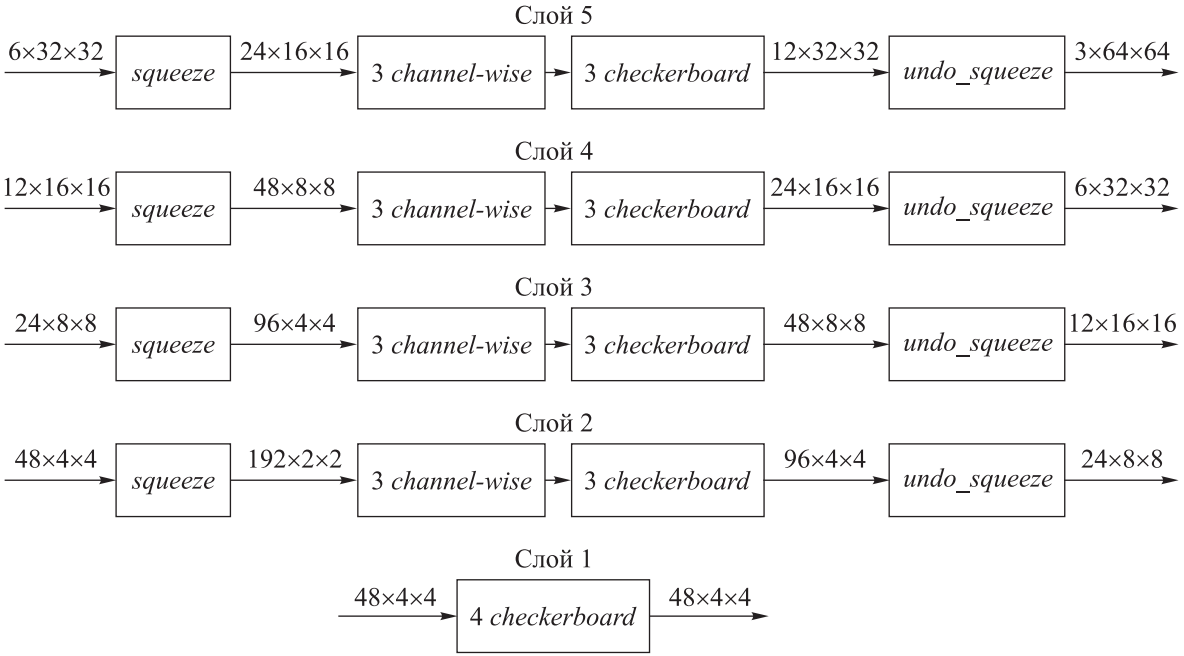
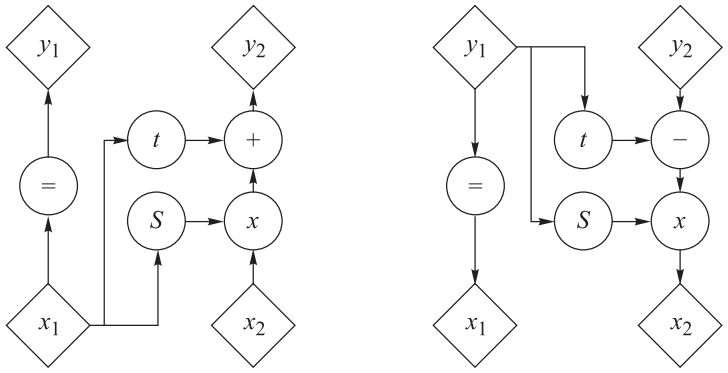


Рис. 7. Схема операции повышения расширения входного изображения

На каждом слое применяются простые обратные преобразования (рис. 8), разделяющие входной вектор на две равные части, одна из которых передается на следующий слой без изменений, а вторая поддается преобразованиям. Фактически, операции кодирования сообщения в изображение, и наоборот, реализуются одними и теми же парными слоями с тем отличием, что вход для декодирования имеет флаг инверсии (*reverse*), позволяющий определить используемый тип операции (операция сложения при кодировании, вычитания при декодировании).



а *б*

Рис. 8. Схемы прямого (*а*) и обратного (*б*) преобразований

Матрица, полученная на выходе, нормируется в диапазоне [0, 255] и сохраняется в виде изображения.

Обработка изображения. В рамках исследования в качестве формата хранения изображения был выбран *tiff*, так как он полностью удовлетворяет требованиям. Основное ограничение — необходимость хранения изображения в контейнере, поддерживающем вещественные числа, что значительно ограничивает доступные форматы изображений.

Алгоритм

Кодировщик

1. Представить входную информацию I в виде массива байт.

2. Проверить возможность сокрытия информации, убедившись, что $sizeOf(I) + KEY \le S$, где $sizeOf$ — функция получения размера входной информации; KEY — заранее заданный размер ключа. Если условие не выполняется, то работа алгоритма останавливается.

3. Сгенерировать массив случайных байт R для последующего сохранения информации.

4. Если размер скрываемого сообщения превышает половину максимального сообщения, то необходимо применить функцию *transform(R, I)*, иначе — функцию *shuffle(R, I)*.

5. Применить линейное нормирование в диапазоне [–1, 1].

6. Представить полученный массив в виде матрицы размером 64 × 64 и подать во входной слой нейронной сети.

7. К полученной матрице применить линейное нормирование в диапазоне [0, 255].

8. Сохранить нормированную матрицу в виде изображения в формате *tiff*.

Декодировщик

1. Представить изображение в формате *tiff* в виде матрицы размером 64 × 64.

2. К полученной матрице применить линейное нормирование в диапазоне [–1, 1].

3. Подать полученную матрицу в инвертированный входной слой нейронной сети.

4. Полученную матрицу нормировать в диапазоне [0, 255] и представить массивом.

5. Определить наличие повторяющихся последовательностей в полученном массиве. Если повторения обнаруживаются и расстояния между ними одинаковые, переход к шагу 6, иначе — к шагу 7.

6. Представить повторяющуюся последовательность в виде массива байт и перейти к шагу 10.

7. Найти в массиве последовательность, соответствующую KEY.

8. Извлечь из массива последовательность от его начала до индекса первого символа последовательности KEY. К полученному срезу применить функцию *transform*.

9. Полученные данные представить байтовым массивом.

10. Сохранить последовательность, исходя из ее MIME-типа. Если тип не определен, то сохранить в виде текста.

Результаты. Рассмотрим несколько примеров работы предлагаемого метода.

1. Скрываемое сообщение «Hello, my name is Maxim. How are you?». Изображение, сгенерированное на основе скрытого сообщения, показано на рис. 9, *а*.

а *б* *в*

Рис. 9. Сгенерированные изображения

2. Скрываемое сообщение «The method includes the stages of preparing input data». Изображение, сгенерированное на основе скрытого сообщения, приведено на рис. 9, *б*.

3. Скрываемое сообщение «The method can serve as a steganographic algorithm for hiding information or an algorithm for adding information in the form of watermarks». Изображение, сгенерированное на основе скрытого сообщения, показано на рис. 9, *в*.

Заключение. Рассмотрены классические стеганографические методы и современные подходы, в том числе основанные на работе нейронных сетей.

Предложен метод, исключающий необходимость использования изображения-контейнера. Метод позволяет генерировать детерминированные изображения с гарантированной возможностью получения исходного сообщения. Основной недостаток предложенного метода — ограниченность поддерживаемых форматов получаемых изображений, что является предметом дальнейших исследований.

ЛИТЕРАТУРА

[1] Грибунин В.Г., Туринцев И.В., Оков И.Н. Цифровая стеганография. М., Солон-Пресс, 2009.

[2] Конахович Г.Ф., Пузыренко А.Ю. Компьютерная стеганография. Теория и практика. Киев, МК-Пресс, 2006.

[3] Das S., Das S., Bandyopadhya B., et al. Steganography and steganalysis: different approaches. *IJCITAE*, 2008, vol. 2, no. 1. DOI: https://doi.org/10.48550/arXiv.1111.3758

[4] Nashat D., Mamdouh L. An efficient steganographic technique for hiding data. *J. Egypt Math. Soc.*, 2019, vol. 27, pp. 57–71.
DOI: https://doi.org/10.1186/s42787-019-0061-6

[5] Kaur H., Ran J. A survey on different techniques of steganography. *MATEC Web Conf.*, 2016, vol. 57, art. 02003. DOI: https://doi.org/10.1051/matecconf/20165702003

[6] Грибунин В.Г., Оков И.Н., Туринцев И.В. Цифровая стеганография. М., Солон-Пресс, 2002.

[7] Zhao J., Koch E. Embedding robust labels into images for copyright protection. *Proc. Int. Cong. on Intellectual Property Rights for Specialized Information, Knowledge and New Techniques*, 1995, pp. 242–251.

[8] Коростиль Ю.М., Шелест М.Е. Принципы построения стеганографических систем со структурной технологией. *Тр. VII Междунар. конф. «Автоматика-2000»*. Ч. 1. Львов, ДНД1П, 2000, с. 273–286.

[9] Joshi K., Gill S., Yadav R. A new method of image steganography using 7th bit of a pixel as indicator by introducing the successive temporary pixel in the gray scale image. *J. Comput. Netw. Commun.*, 2018, vol. 2018, art. 9475142.
DOI: https://doi.org/10.1155/2018/9475142

[10] Tiwari R.K., Sahoo G. Some new methodologies for image hiding using steganographic techniques. *Cryptography and Security*.
DOI: https://doi.org/10.48550/arXiv.1211.0377

[11] Bandyopadhyay S.K. Advisor to chancellor. A proposed method for image steganography. *Res. Med. Eng. Sci*., 2018, vol. 3, no. 4, art. RMES.000569.2018.
DOI: http://dx.doi.org/10.31031/rmes.2018.03.000569

[12] Hayes J., Danezis G. Generating steganographic images via adversarial training. *Proc. NIPS*, 2017, pp. 1951–1960.

[13] Zhang K.A., Cuesta-Infante A., Xu L., et al. SteganoGAN: high capacity image steganography with GANs. DOI: https://doi.org/10.48550/arXiv.1901.03892

[14] Dinh L., Sohl-Dickstein J., Bengio S. Density estimation using Real NVP. *ICLR*, 2017. DOI: https://doi.org/10.48550/arXiv.1605.08803

[15] Dinh L., Krueger D., Bengio Y. NICE: non-linear independent components estimation. *ICLR*, 2015. DOI: https://doi.org/10.48550/arXiv.1410.8516

Рудаков Игорь Владимирович — канд. техн. наук, заведующий кафедрой «Программное обеспечение ЭВМ и информационные технологии» МГТУ им. Н.Э. Баумана (Российская Федерация, 105005, Москва, 2-я Бауманская ул., д. 5, стр. 1).

Филиппов Михаил Владимирович — канд. техн. наук, доцент кафедры «Программное обеспечение ЭВМ и информационные технологии» МГТУ им. Н.Э. Баумана (Российская Федерация, 105005, Москва, 2-я Бауманская ул., д. 5, стр. 1).

Кудрявцев Максим Александрович — аспирант кафедры «Программное обеспечение ЭВМ и информационные технологии» МГТУ им. Н.Э. Баумана (Российская Федерация, 105005, Москва, 2-я Бауманская ул., д. 5, стр. 1).

Просьба ссылаться на эту статью следующим образом:

Рудков И.В., Филиппов М.В., Кудрявцев М.А. Метод генерации изображений с использованием нейронных сетей на основе восстанавливаемой байтовой последовательности. *Вестник МГТУ им. Н.Э. Баумана. Сер. Приборостроение*, 2023, № 1 (142), с. 83–97. DOI: https://doi.org/10.18698/0236-3933-2023-1-83-97

IMAGE GENERATION METHOD BASED ON THE RECOVERABLE BYTE SEQUENCE USING THE NEURAL NETWORKS

I.V. Rudakov irudakov@bmstu.ru
M.V. Filippov filippovmv@bmstu.ru
M.A. Kudryavtsev kudryavtsev@bmstu.ru

Bauman Moscow State Technical University, Moscow, Russian Federation

Abstract

Due to the rapid development of information technologies, the tasks of ensuring information integrity, safety and confidentiality, as well as the possibility of guaranteed confirmation of its source, are becoming more relevant than ever. One of the possible solutions to this problem could be the steganographic methods, which allow both hiding the fact of information transfer and imperceptibly adding the useful data. Scientific literature describes a large number of steganographic algorithms. However, only insignificant number of works is devoted to the data hiding methods using the neural networks, and even less are devoted to generating containers for them. A method for generating images based on the hidden information is proposed, which guarantees possibility of both hiding and subsequent extraction of information eliminating the need to select an appropriate container. As part of the method, an algorithm was developed that included description of the stages of input data preprocessing, transformation into the container image and extraction of the hidden information. Examples of the proposed method operation are provided. The method could serve both as a steganographic algorithm for hiding information and as the algorithm for adding information in the form of watermarks

Keywords

Steganography, information hiding, watermarks, image generation, neural networks

Received 05.04.2022
Accepted 08.11.2022

REFERENCES

[1] Gribunin V.G., Turintsev I.V., Okov I.N. Tsifrovaya steganografiya [Digital steganography]. Moscow, Solon-Press Publ., 2009.

[2] Konakhovich G.F., Puzyrenko A.Yu. Kompyuternaya steganografiya. Teoriya i praktika [Computer steganography. Theory and practice]. Kiev, MK-Press Publ., 2006.

[3] Das S., Das S., Bandyopadhya B., et al. Steganography and steganalysis: different approaches. *IJCITAE*, 2008, vol. 2, no. 1. DOI: https://doi.org/10.48550/arXiv.1111.3758

[4] Nashat D., Mamdouh L. An efficient steganographic technique for hiding data. *J. Egypt Math. Soc*., 2019, vol. 27, pp. 57–71.
DOI: https://doi.org/10.1186/s42787-019-0061-6

[5] Kaur H., Ran J. A survey on different techniques of steganography. *MATEC Web Conf*., 2016, vol. 57, art. 02003. DOI: https://doi.org/10.1051/matecconf/20165702003

[6] Gribunin V.G., Okov I.N., Turintsev I.V. Tsifrovaya steganografiya [Digital steganography]. Moscow, Solon-Press Publ., 2002.

[7] Zhao J., Koch E. Embedding robust labels into images for copyright protection. *Proc. Int. Cong. on Intellectual Property Rights for Specialized Information, Knowledge and New Techniques*, 1995, pp. 242–251.

[8] Korostil Yu.M., Shelest M.E. [Design principles of steganographic systems with structural technology]. *Tr. VII Mezhdunar. konf. "Avtomatika-2000". Ch. 1* [Proc. VII Int. Conf. Automatics-2000. P. 1]. Lvov, DND1P Publ., 2000, pp. 273–286 (in Russ.).

[9] Joshi K., Gill S., Yadav R. A new method of image steganography using 7th bit of a pixel as indicator by introducing the successive temporary pixel in the gray scale image. *J. Comput. Netw. Commun.*, 2018, vol. 2018, art. 9475142.
DOI: https://doi.org/10.1155/2018/9475142

[10] Tiwari R.K., Sahoo G. Some new methodologies for image hiding using steganographic techniques. *Cryptography and Security*.
DOI: https://doi.org/10.48550/arXiv.1211.0377

[11] Bandyopadhyay S.K. Advisor to chancellor. A proposed method for image steganography. *Res. Med. Eng. Sci*., 2018, vol. 3, no. 4, art. RMES.000569.2018.
DOI: http://dx.doi.org/10.31031/rmes.2018.03.000569

[12] Hayes J., Danezis G. Generating steganographic images via adversarial training. *Proc. NIPS*, 2017, pp. 1951–1960.

[13] Zhang K.A., Cuesta-Infante A., Xu L., et al. SteganoGAN: high capacity image steganography with GANs. DOI: https://doi.org/10.48550/arXiv.1901.03892

[14] Dinh L., Sohl-Dickstein J., Bengio S. Density estimation using Real NVP. *ICLR*, 2017. DOI: https://doi.org/10.48550/arXiv.1605.08803

[15] Dinh L., Krueger D., Bengio Y. NICE: non-linear independent components estimation. *ICLR*, 2015. DOI: https://doi.org/10.48550/arXiv.1410.8516

Rudakov I.V. — Cand. Sc. (Eng.), Head of the Department of Computer Software and Information Technologies, Bauman Moscow State Technical University (2-ya Baumanskaya ul. 5, str. 1, Moscow, 105005 Russian Federation).

Filippov M.V. — Cand. Sc. (Eng.), Assoc. Professor, Department of Computer Software and Information Technologies, Bauman Moscow State Technical University (2-ya Baumanskaya ul. 5, str. 1, Moscow, 105005 Russian Federation).

Kudryavtsev M.A. — Post-Graduate Student, Department of Computer Software and Information Technologies, Bauman Moscow State Technical University (2-ya Baumanskaya ul. 5, str. 1, Moscow, 105005 Russian Federation).

Please cite this article in English as:

Rudakov I.V., Filippov M.V., Kudryavtsev M.A. Image generation method based on the recoverable byte sequence using the neural networks. *Herald of the Bauman Moscow State Technical University, Series Instrument Engineering*, 2023, no. 1 (142), pp. 83–97 (in Russ.). DOI: https://doi.org/10.18698/0236-3933-2023-1-83-97