УНИВЕРСИТЕТ ИТМО
НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ
май–июнь 2017 Том 17 № 3 ISSN 2226-1494 http://ntv.ifmo.ru/
SCIENTIFIC AND TECHNICAL JOURNAL OF INFORMATION TECHNOLOGIES, MECHANICS AND OPTICS
May–June 2017 Vol. 17 No 3 ISSN 2226-1494 http://ntv.ifmo.ru/en

УДК 004.056.5

ЭФФЕКТИВНОСТЬ СТЕГАНОАНАЛИЗА НА ОСНОВЕ МЕТОДОВ МАШИННОГО ОБУЧЕНИЯ

А.В. Сивачев[a], Н.Н. Прохожев[a], О.В. Михайличенко[a], Д.А. Башмаков[a]

[a] Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация
Адрес для переписки: 19791109@list.ru

Информация о статье
Поступила в редакцию 02.03.17, принята к печати 26.04.17
doi: 10.17586/2226-1494-2017-17-3-457-466
Язык статьи – русский

Ссылка для цитирования: Сивачев А.В., Прохожев Н.Н., Михайличенко О.В., Башмаков Д.А. Эффективность стеганоанализа на основе методов машинного обучения // Научно-технический вестник информационных технологий, механики и оптики. 2017. Т. 17. № 3. С. 457–466. doi: 10.17586/2226-1494-2017-17-3-457-466

Аннотация

Предмет исследования. Проведена сравнительная оценка точности методов стеганоанализа на основе машинного обучения в задачах пассивного противодействия каналам передачи данных, использующим область дискретного вейвлет-преобразования неподвижных цифровых изображений. **Методы.** Исследованы методы авторов Gireesh Kumar, Hany Farid, Changxin Liu, Yun Q. Shi и SPAM. В основу методов стеганоанализа положено использование статистических моментов, полученных для областей LL, HL, LH и HH при дискретном вейвлет-преобразовании, и дополнительных параметров изображения, составляющих опорный вектор. Для оценки методов использована коллекция изображений BOWS2. Встраивание информации смоделировано путем изменения значений младших бит коэффициентов каждой из областей дискретного вейвлет-преобразования изображения (LL, LH, HL, HH) с 5% и 20% полезной нагрузки. Эффективность методов определена с учетом полученных истинно положительных, истинно отрицательных, ложноположительных и ложноотрицательных значений классификации изображений. **Основные результаты**. Показано, что все методы, за исключением SPAM, эффективны при обнаружении встраивания информации в HH область. При обнаружении факта встраивания информации в область LH эффективным методом является Yun Q. Shi. При обнаружении факта встраивания в HL область все методы, кроме SPAM, оказались сравнительно эффективными, но при большом объеме полезной нагрузки. При обнаружении факта встраивания в LL область все методы показали эффективность около 50% независимо от объема полезной нагрузки. Установлено, что рассмотренные методы не в состоянии оказать эффективное противодействие скрытому каналу передачи данных, использующему LH и HL области, в связи с тем, что они используют вейвлет-преобразование Хаара. Сделан вывод, что применение оптимального вейвлет-преобразования позволит максимально уменьшить область пересечения гистограмм значений первого статистического момента для оригинальных изображений и стеганоизображений. **Практическая значимость.** Результаты работы полезны специалистам в области защиты информации в задачах обнаружения и противодействия скрытым каналам передачи данных. Полученные результаты могут быть использованы при разработке систем стеганоанализа, а также для разработки усовершенствованных методов стеганоанализа.

Ключевые слова

стеганография, машинное обучение, пассивное противодействие, скрытый канал передачи, система и алгоритмы стеганоанализа, бинарная классификация, низкочастотная область одномерного ДВП, дискретное вейвлет-преобразование, преобразование Хаара и Добеши, младший значащий бит

EFFECTIVENESS OF STEGANALYSIS BASED ON MACHINE LEARNING METHODS

A.M. Sivachev[a], N.N. Prokhozhev[a], O.V. Mikhailichenko[a], D.A. Bashmakov[a]

[a] ITMO University, Saint Petersburg, 197101, Russian Federation
Corresponding author: 19791109@list.ru

Article info
Received 02.03.17, accepted 26.04.17
doi: 10.17586/2226-1494-2017-17-3-457-466
Article in Russian

For citation: Sivachev A.M., Prokhozhev N.N., Mikhailichenko O.V., Bashmakov D.A. Effectiveness of steganalysis based on machine learning methods. *Scientific and Technical Journal of Information Technologies, Mechanics and Optics*, 2017, vol. 17, no. 3, pp. 457–466 (in Russian). doi: 10.17586/2226-1494-2017-17-3-457-466

Abstract

Subject of Study. The paper presents comparative accuracy estimation of modern machine learning-based steganalytic methods. The paper deals with the most perspective methods in tasks of the passive counteraction to the information transfer channels using the discrete wavelet domain of static digital images. **Methods.** We have studied methods proposed by Gireesh Kumar, Hany Farid, Changxin Liu, Yun Q. Shi and the SPAM method. Basically the methods apply statistical moments obtained from wavelet bands LL, HL, LH and HH, as well as additional image features forming a support vector. BOWS2 image collection was used to estimate the effectiveness of methods. Steganographic impact was modeled by changing the least significant bits of coefficients for the each DWT band (LL, LH, HL and HH) with 5% and 20% of payload. The effectiveness of explored methods is estimated in view of obtained true positive, true negative, false positive and false negative image classification values. **Main Results.** The study has shown that all explored methods except for SPAM are effective in the task of detecting of embedding in HH band. As for the detection of the embedding in LH band, Yun Q. Shi is the most effective algorithm. In the task of the detecting in HL band, all explored methods except for SPAM have appeared to be comparatively effective under condition of big payload. When detecting the embedding in LL band, all methods have shown the effectiveness about 50% regardless the payload rate. It is established that the considered methods are not able to render effective counteraction to the hidden data channel, using the LH and HL region due to the fact that they use Haar wavelet transform. It is concluded that the application of the optimal wavelet transform makes it possible to reduce the intersection area of value histograms of the first statistical moment for the original images and steganoimages. **Practical Relevance.** The work results are useful to the specialists in the field of information security in the tasks of detection and combating the hidden data channels. The obtained results can be used in the development of steganalysis systems and improved methods of steganalysis as well.

Keywords

steganography, machine learning, passive counteraction, hidden channel, steganalisys system and algorithms, binary classification, one-dimensional DWT low-frequency region, discrete wavelet transform, Haar and Daubechies transform, least significant bit

Введение

В современном глобальном информационном пространстве стеганография может быть успешно использована в задачах организации скрытых каналов передачи информации [1], а также ряде других задач [2]. Применение стеганографии для создания скрытых каналов передачи информации все чаще встречается в деятельности как криминальных или террористических организаций [3], так и правительственных спецслужб [4]. Неподвижные изображения являются одним из распространенных типов стеганографических контейнеров, использующихся для сокрытия информации и имеющих большое количество методов встраивания [5].

В целях пассивного противодействия скрытым каналам передачи информации на основе дискретного вейвлет-преобразования (ДВП) разрабатываются методы стеганоанализа, позволяющие определить факт сокрытия информации в изображении. К сожалению, на данный момент отсутствуют универсальные методы стеганоанализа, позволяющие с высокой степенью вероятности и независимо от используемого стеганографического метода обнаружить факт встраивания. Например, статистические количественные методы стеганоанализа позволяют с высокой точностью определить количество пикселей изображения, значения младших бит которых были изменены в результате встраивания информации [6, 7]. В то же время эти методы оказываются неэффективны при обнаружении факта встраивания информации в область младших бит ДВП-коэффициентов изображения.

Существует множество методов стеганоанализа, которые различаются по используемым характеристикам изображения и методам встраивания, которым они противодействуют. Использование методов на основе машинного обучения является перспективным направлением в области стеганоанализа [8].

При практическом решении задачи пассивного противодействия скрытым каналам передачи информации основным критерием выбора метода стеганоанализа является его эффективность. В данной работе для методов стеганоанализа на основе машинного обучения в качестве оценки эффективности принимаются параметры точности бинарной классификации. В случае со встраиванием информации в коэффициенты ДВП для метода стеганоанализа также имеет значение его точность для различных областей коэффициентов ДВП, так как при одноуровневом вейвлет-разложении получаются четыре области коэффициентов, которые содержат высоко- (D, H, V) или низкочастотную (A) составляющую цифрового изображения.

Среди опубликованных исследований практически отсутствуют работы, в которых проводится сравнение существующих методов стеганоанализа на основе машинного обучения. В основном информация о точности метода стеганоанализа предоставляется самими авторами метода при его описании. Однако провести сравнение методов стеганоанализа, основываясь на заявленных самими авторами данных, достаточно сложно, так как авторы используют разные коллекции изображений и разные методы встраивания информации в изображение. Исходя из этого, исследования, позволяющие провести сравнительную оценку эффективности различных современных методов стеганоанализа в одинаковых условиях, являются актуальными и могут быть использованы при практической организации пассивного противодействия стеганографии, а также с целью дальнейшего совершенствования методов стеганоанализа.

В работе проводится сравнительная оценка точности рассматриваемых методов стеганоанализа с учетом создания равных условий (одинаковая полезная нагрузка, выборка изображений и метод встраивания). Результаты оценки позволяют выбрать оптимальный метод для пассивного противодействия скрытым каналам передачи информации, использующих области коэффициентов ДВП цифровых изображений.

Методика исследования

Из современных методов стеганоанализа на основе машинного обучения для исследования были выбраны следующие методы, широко известные и наиболее часто цитируемые:
- метод, предложенный Gireesh Kumar и др. [9];
- метод, предложенный Hany Farid [10];
- метод, предложенный Changxin Liu и др. [11];
- метод SPAM (Subtractive Pixel Adjacency Model) [12];
- метод, предложенный Yun Q. Shi и др. [13].

Авторами настоящей работы был проведен сравнительный анализ набора параметров, используемых каждым из методов [9–13]. Большинство выбранных методов стеганоанализа, кроме [10], для обнаружения факта встраивания информации используют статистические моменты, полученные для областей LL, HL, LH и HH при ДВП изображения. Основная разница между рассматриваемыми методами заключается в количестве уровней вейвлет-преобразования, а также в используемых дополнительных параметрах изображения, составляющих опорный вектор. С учетом описания [9–13] в табл. 1 приведено сравнение основных и дополнительных параметров, используемых методами стеганоанализа.

Метод стеганоанализа	Уровень ДВП	Статистические моменты	Дополнительные параметры
Gireesh Kumar	3	1, 2, 3 и 4	Не используются
Hany Farid	4	1, 2, 3 и 4	Оценка погрешности между реальными и предсказанными значениями коэффициентов областей HL, LH и HH (по приведенной авторами метода формуле)
Changxin Liu	3	1, 2, 3 и 4	Градиентная энергия и энтропия изображения, а также оценка погрешности между реальными и предсказанными значениями коэффициентов областей HL, LH и HH (по приведенной авторами метода формуле)
SPAM	Не используются	Не используется	Матрица разницы соседних пикселей, рассчитанная на основе цепей Маркова
Yun Q. Shi	2	1, 2 (по формулам, представленным в работе)	Не используются

Таблица 1. Сравнение основных и дополнительных параметров, используемых методами стеганоанализа

На основе имеющегося тестового множества цифровых изображений формируется подмножество оригинальных изображений и подмножество стеганоизображений. Для стеганоизображений моделируется встраивание информации путем модификации фиксированного процента коэффициентов (полезная нагрузка) определенной области ДВП-изображения. После этого для изображений из тестового множества производится расчет параметров, используемых для классификации изображений конкретным методом стеганоанализа. Полученные для оригинальных и стеганоизображений параметры разбиваются на две выборки: обучающую и тестовую. Сначала для конкретного метода стеганоанализа метод машинного обучения обучается на обучающей выборке, после чего точность обученного классификатора проверяется с использованием тестовой выборки. Полученные результаты сохраняются для дальнейшей обработки и сравнения различных методов стеганоанализа.

Для проведения экспериментов была выбрана коллекция изображений BOWS2 [14], используемая в качестве основной коллекции для тестирования методов стеганоанализа. Эта коллекция была выбрана в связи с тем, что она:
- достаточно известна и часто используется разными авторами в работах по стеганографии [12, 15, 16];
- насчитывает большое количество (более 1000) изображений разрешением 512×512 пикселей;
- находится в свободном доступе.

Для формирования обучающей выборки из коллекции BOWS2 использовалось 20% изображений. Остальные 80% изображений коллекции использовались в качестве тестовой выборки. В каждой выборке количество оригинальных изображений и стеганоизображений было равным.

Встраивание информации осуществлялось путем изменения значений младших бит коэффициентов каждой из четырех областей (LL, LH, HL, HH) при одноуровневом ДВП.

Для оценки степени искажения исходного контейнера, возникающего при встраивании информации, была проведена оценка среднего арифметического значения PSNR (peak signal to noise ratio – пиковое отношение сигнала к шуму) для используемой коллекции изображений. В табл. 2 для коллекции изображений BOWS2 приведены рассчитанные значения PSNR в зависимости от объема встраивания.

Область встраивания	Объем встраивания,%	Среднее арифметическое значение PSNR
LL	5	61,1
	10	58,1
	15	56,4
	20	55,1
HH	5	61,2
	10	58,2
	15	56,4
	20	55,1
LH	5	61,2
	10	58,2
	15	56,4
	20	55,1
HL	5	61,2
	10	58,2
	15	56,4
	20	55,1

Таблица 2. Значения PSNR для изображений коллекции BOWS2 в зависимости от объема встраивания

Эффективность исследуемых методов стеганоанализа определяется корректностью классификации изображений – оригинальное изображение или стеганоизображение. Для идеального метода стеганоанализа 100% изображений, содержащих встроенную информацию, должны быть классифицированы как стеганоизображение, а 100% изображений, не содержащих встроенную информацию, должны быть классифицированы как оригинальные изображения. Точность реального классификатора, использующего рассматриваемые методы стеганоанализа, всегда будет иметь некоторую погрешность. Таким образом, оценка результата классификации может иметь четыре значения: истинно положительное (TP), истинно отрицательное (TN), ложноположительное (FP) и ложноотрицательное (FN). Наглядно сравнить точность нескольких методов стеганоанализа можно с помощью графика соотношения значений TN, TP, FP, FN, T=TN+TP и F=FP+FN, где по оси *Y* располагается количество изображений в процентах, классифицированных соответствующим образом от общего количества.

Результаты исследования

Для наглядного сравнения исследуемых в работе методов стеганоанализа результаты классификации при обучении на стеганоизображениях с полезной нагрузкой 5% представлены в виде графиков значений TN, TP, FP, FN, T, F на рис. 1–4, а с полезной нагрузкой 20% – на рис. 5–8. Поскольку количество стеганоизображений и оригинальных изображений в выборке было равным, то идеальный классификатор имел бы следующие значения: 50% TP, 50% TN, 0% FP, 0% FN, 100% T, 0% F.

На рис. 1–8 видно, что большинство исследуемых методов стеганоанализа оказывается достаточно эффективным при обнаружении встраивания информации в HH область изображения – более 90% верно классифицированных изображений при объеме полезной нагрузки в 5% и более 97% при объеме полезной нагрузки в 20%. Исключением является метод SPAM, принцип работы которого основан на матрице разностей соседних пикселей: он разрабатывался в основном для противодействия LSB-встраиванию в пространственную область изображения.

При обнаружении факта встраивания в область LH большинство методов оказались неэффективными – 50%–60% верно классифицированных изображений. Единственным эффективным является метод Yun Q. Shi, отличающийся относительной простотой и показавший эффективность около 80%–90% верно классифицированных изображений.

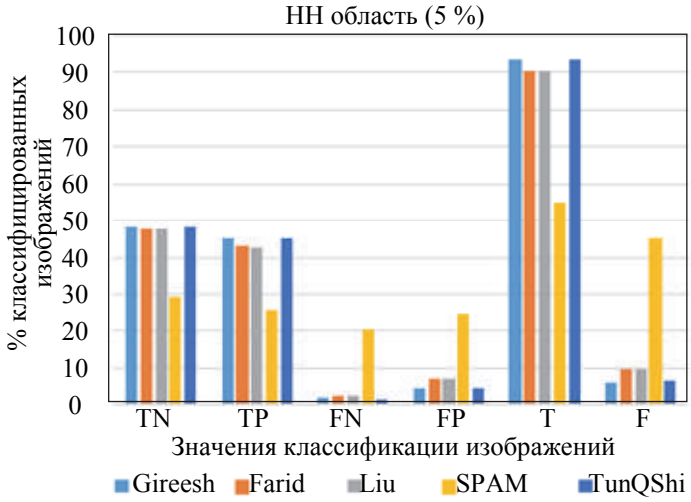

Рис. 1. Соотношение TN, TP, FP, FN, T, F при встраивании в HH область (полезная нагрузка 5%)

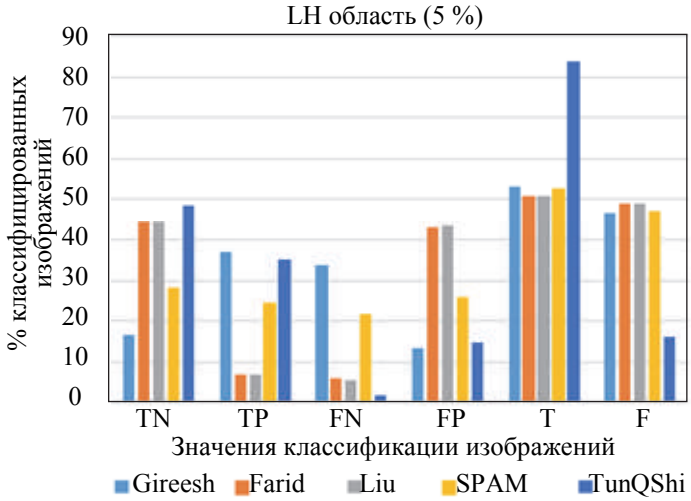

Рис. 2. Соотношение TN, TP, FP, FN, T, F при встраивании в LH область (полезная нагрузка 5%)

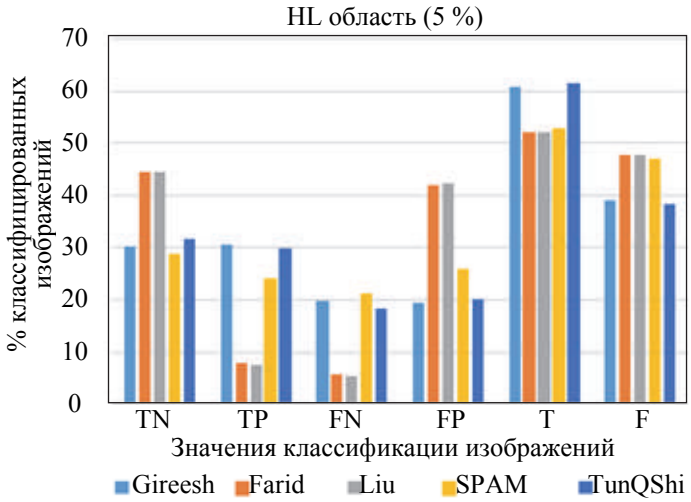

Рис. 3. Соотношение TN, TP, FP, FN, T, F при встраивании в HL область (полезная нагрузка 5%)

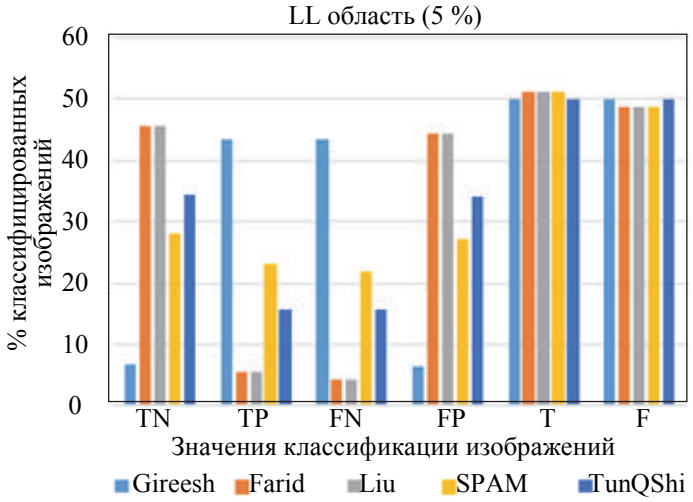

Рис. 4. Соотношение TN, TP, FP, FN, T, F при встраивании в LL область (полезная нагрузка 5%)

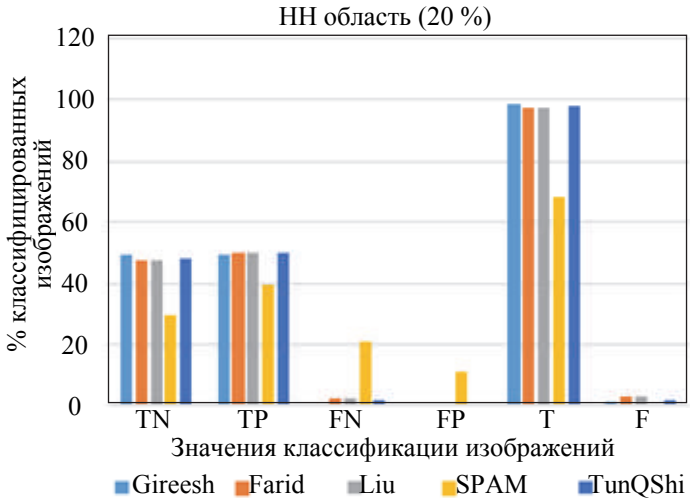

Рис. 5. Соотношение TN, TP, FP, FN, T, F при встраивании в HH область (полезная нагрузка 20%)

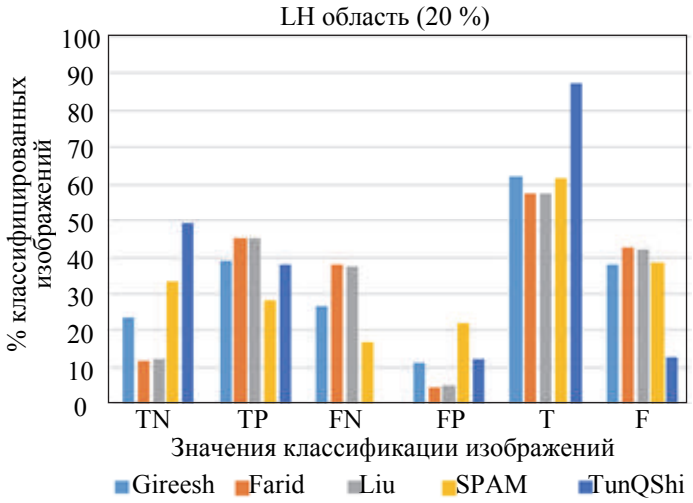

Рис. 6. Соотношение TN, TP, FP, FN, T, F при встраивании в LH область (полезная нагрузка 20%)

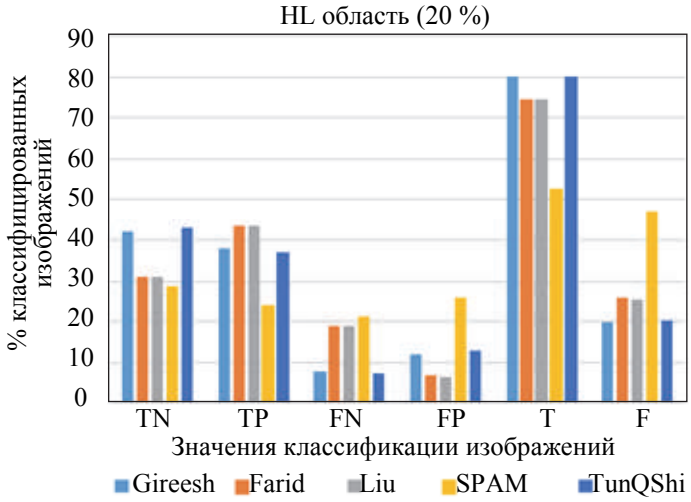

Рис. 7. Соотношение TN, TP, FP, FN, T, F при встраивании в HL область (полезная нагрузка 20%)

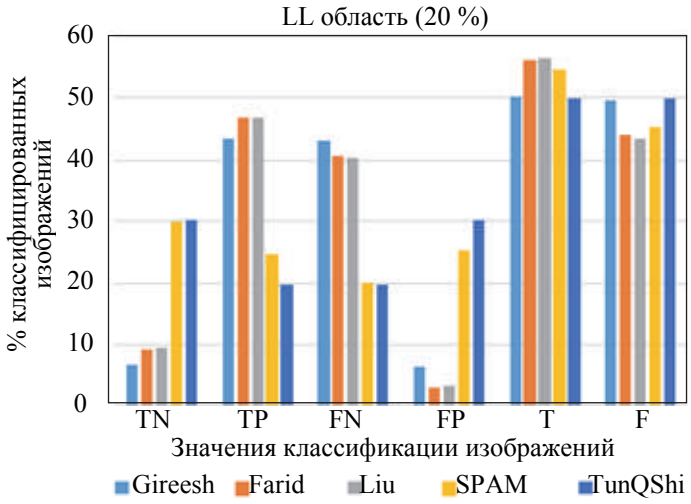

Рис. 8. Соотношение TN, TP, FP, FN, T, F при встраивании в LL область (полезная нагрузка 20%)

Для HL области все методы, кроме SPAM, оказались сравнительно эффективными, но только при достаточно большом объеме полезной нагрузки –75%–80% верно классифицированных изображений при 20% полезной нагрузке (при 5% полезной нагрузке процент верно классифицированных изображений составил только 50%–60%).

При обнаружении факта встраивания в LL область все методы показали эффективность около 50% независимо от объема полезной нагрузки, что на практике обозначает отсутствие возможности различить оригинальные и стеганоизображения при встраивании в эту область.

Обсуждение результатов

Современные методы стеганоанализа на основе методов машинного обучения позволяют определить стеганоизображение со встраиванием в HH область коэффициентов ДВП при полезной нагрузке пять и более процентов. Результаты работы алгоритмов, предложенных в [9, 13], показали высокую эффективность при классификации оригинальных и стеганоизображений для HH области.

Точность детектирования факта встраивания скрытой информации исследуемыми методами стеганоанализа для LH и HL областей коэффициентов ДВП значительно уступает аналогичному параметру для области HH, что не позволяет организовать эффективное пассивное противодействие скрытым каналам передачи информации с полезной нагрузкой менее 15%–20%.

Результаты, полученные для LL области коэффициентов ДВП, показывают практическую невозможность детектирования факта встраивания скрытой информации. При этом стоит отметить, что изменения, вносимые при встраивании информации в низкочастотную область изображения, могут приводить к визуализации артефактов встраивания. По этой причине низкочастотная область ДВП в задачах сокрытия информации используется не так часто, как высокочастотные области.

Вышеописанные результаты можно объяснить тем обстоятельством, что рассматриваемые алгоритмы в своей основе используют вейвлет-преобразование Хаара. Проведенные дополнительные исследования показали, что получаемые значения статистических моментов, выступающих в роли параметров для опорных векторов, имеют значительный разброс величин. Это неизбежно приводит к тому, что множества значений для оригинальных и стеганоизображений пересекаются (рис. 9, а) что, как следствие, затрудняет классификацию изображения по данным параметрам. Результаты исследования, проведенного для вейвлет-преобразования Добеши (рис. 9, б), показали, что область пересечения гистограмм значений первого статистического момента для HL области оригинальных и стегано-изображений значительно уменьшилась, что дает хорошие перспективы для машинного обучения.

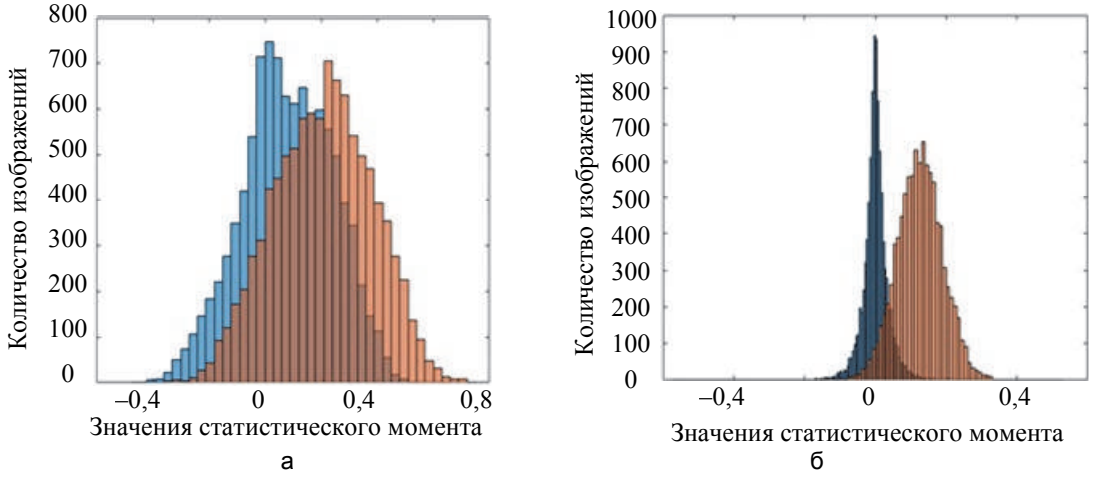

Рис. 9. Гистограмма значений первого статистического момента для HL области оригинальных (синий) и стеганоизображений (оранжевый) при использовании вейвлет-преобразований: Хаара (а); Добеши (б)

Одним из недостатков рассматриваемых алгоритмов является игнорирование известных зависимостей между значениями коэффициентов различных областей вейвлет-преобразования. На рис. 10 приведен график зависимости первого статистического момента для HL области двумерного вейвлет-преобразования (рис. 9, а) от статистического момента, полученного с использованием низкочастотной области одномерного вейвлет-преобразования для оригинального изображения.

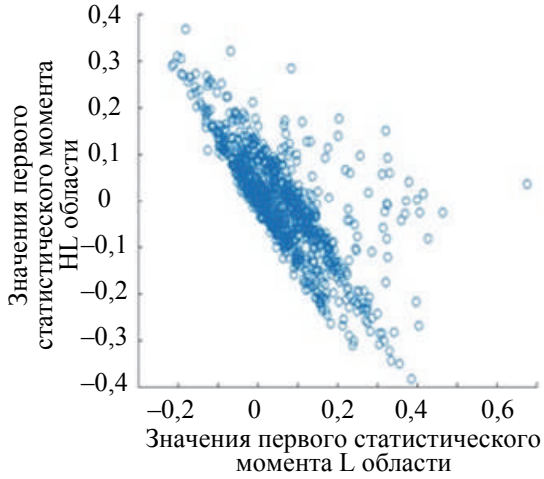

Рис. 10. Зависимость первого статистического момента для HL области от статистического момента, полученного с использованием низкочастотной области одномерного вейвлет-преобразования

При изменении коэффициентов HL области низкочастотная область одномерного преобразования не претерпевает значимых изменений. Учитывая взаимосвязь между этими двумя областями вейвлет-преобразования, можно фиксировать аномалии отклонения значений параметра первого статистического момента, вызванного встраиванием информации в коэффициенты HL области двумерного вейвлет-преобразования, и упростить задачу классификации изображений.

Заключение

В работе проведено исследование эффективности методов стеганоанализа на основе машин опорных векторов. Результаты исследования показали, что исследуемые методы стеганоанализа не в состоя-

нии оказать эффективное противодействие в отношении стеганоканала, использующего LH и HL области коэффициентов дискретного вейвлет-преобразования. Так, при одноуровневом разложении для изображения размером 512×512 пикселей получается четыре области коэффициентов дискретного вейвлет-преобразования: LL, LH, HL и HH. Каждая область имеет размер 256×256 коэффициентов. В LH и HL области может быть произведено встраивание с полезной нагрузкой до 10%–15%, что обеспечит пропускную способность стеганоканала даже в условиях пассивного противодействия в 1,5–2,5 кБ.

Необходимо дальнейшее совершенствование методов стеганоанализа для обнаружения факта встраивания в область дискретного вейвлет-преобразования изображения. Такое совершенствование возможно по следующим направлениям:

1. выбор оптимального вейвлет-преобразования, которое позволит максимально уменьшить область пересечения гистограмм значений первого статистического момента для оригинальных изображений и стеганоизображений;
2. поиск и использование дополнительных параметров изображения для формирования опорных векторов, позволяющих повысить однозначность разделения множества оригинальных изображений и стеганоизображений.

Литература

1. Грибунин В.Г., Оков И.Н., Туринцев И.В. Цифровая стеганография. М.: Солон-Пресс, 2016. 262 с.
2. Макаренко С.И. Эталонная модель взаимодействия стеганографических систем и обоснование на ее основе новых направлений развития теории стеганографии // Вопросы кибербезопасности. 2014. № 2. С. 24–32.
3. Steganography: A Powerful Tool for Terrorists and Corporate Spies // Stratfor [Электронный ресурс]. Режим доступа: https://www.stratfor.com/analysis/steganography-powerful-tool-terrorists-and-corporate-spies, свободный. Яз. англ. (дата обращения 02.02.2017).
4. Kessler G.C. An overview of steganography for the computer forensics examiner // Forensic Science Communications. 2004. V. 6. N 3.
5. Gayathri C., Kalpana V. Study on image steganography techniques // International Journal of Engineering and Technology. 2013. V. 5. N 2. P. 572–577.
6. Prokhozhev N., Mikhailichenko O., Sivachev A., Bashmakov D., Korobeynikov A.G. Passive steganalysis evaluation: reliabilities of modern quantitative steganalysis algorithms // Advances in Intelligent Systems and Computing. 2016. V. 451. P. 89–94. doi:10.1007/978-3-319-33816-3_9
7. Прохожев Н.Н., Михайличенко О.В., Башмаков Д.А., Сивачев А.В., Коробейников А.Г. Исследование эффективности применения статистических алгоритмов количественного стеганоанализа в задаче детектирования скрытых каналов передачи информации // Программные системы и вычислительные методы. 2015. № 3. С. 281–292. doi: 10.7256/2305-6061.2015.3.17233
8. Schaathun H.G. Machine Learning in Image Steganalysis. Wiley-IEEE Press, 2012. 290 p.
9. Gireesh Kumar T., Jithin R., Shankar D.D. Feature based steganalysis using wavelet decomposition and magnitude statistics // Proc. Int. Conf. on Advances in Computer Engineering. Bangalore, India, 2010. P. 298–300. doi: 10.1109/ACE.2010.33
10. Hany F. Detecting Steganographic Messages in Digital Images. Technical Report TR2001-412, Dartmouth College, 2001.
11. Liu C., Ouyang C., Guo M., Chen H. Image steganalysis based on spatial domain and DWT domain features // Proc. 2nd Int. Conf. on Networks Security, Wireless Communications and Trusted Computing. 2010. V. 1. P. 329–331. doi: 10.1109/NSWCTC.2010.271
12. Pevny T., Bas P., Fredrich J. Steganalysis by subtractive pixel adjacency matrix // IEEE Transactions on Information Forensics and Security. 2010. V. 5. N 2. P. 215–224. doi: 10.1109/TIFS.2010.2045842
13. Shi Y.Q., Xuan G., Yang C., Gao J., Zhang Z., Chai P., Zou D., Chen C., Chen W. Effective steganalysis based on statistical moments of wavelet characteristic function // Proc. Int. Conf. on Information Technology: Coding and Computing (ITCC'05). Las Vegas, USA, 2005. V. 2. P. 768–773.
14. BOWS2 the 10 000 original images [Электронный ресурс].

References

1. Gribunin V.G., Okov I.N., Turintsev I.V. *Digital Steganography*. Moscow, SOLON-Press, 2016, 262 p. (In Russian)
2. Makarenko S. The steganographic system interconnection basic reference model and the justification of new areas of steganography theory's development. *Voprosy Kiberbezopasnosti*, 2014, no. 2, pp. 24–32. (In Russian)
3. *Steganography: A Powerful Tool for Terrorists and Corporate Spies*. Stratfor. Available at: https://www.stratfor.com/analysis/steganography-powerful-tool-terrorists-and-corporate-spies (accessed 02.02.2017).
4. Kessler G.C. An overview of steganography for the computer forensics examiner. *Forensic Science Communications*, 2004, vol. 6, no. 3.
5. Gayathri C., Kalpana V. Study on image steganography techniques. *International Journal of Engineering and Technology*, 2013, vol. 5, no. 2, pp. 572–577.
6. Prokhozhev N., Mikhailichenko O., Sivachev A., Bashmakov D., Korobeynikov A.G. Passive steganalysis evaluation: reliabilities of modern quantitative steganalysis algorithms. *Advances in Intelligent Systems and Computing*, 2016, vol. 451, pp. 89–94. doi:10.1007/978-3-319-33816-3_9
7. Prokhozhev N.N., Mikhailichenko O.V., Bashmakov D.A., Sivachev A.V., Korobeinikov A.G. Software Study the effectiveness of statistical algorithms of quantitative steganalysis in the task of detecting hidden information channels. *Systems and Computational Methods*, 2015, no. 3, pp. 281–292. (In Russian) doi: 10.7256/2305-6061.2015.3.17233
8. Schaathun H.G. *Machine Learning in Image Steganalysis*. Wiley-IEEE Press, 2012, 290 p.
9. Gireesh Kumar T., Jithin R., Shankar D.D. Feature based steganalysis using wavelet decomposition and magnitude statistics. *Proc. Int. Conf. on Advances in Computer Engineering*. Bangalore, India, 2010, pp. 298–300. doi: 10.1109/ACE.2010.33
10. Hany F. Detecting Steganographic Messages in Digital Images. *Technical Report TR2001-412*, Dartmouth College, 2001.
11. Liu C., Ouyang C., Guo M., Chen H. Image steganalysis based on spatial domain and DWT domain features. *Proc. 2nd Int. Conf. on Networks Security, Wireless Communications and Trusted Computing*, 2010, vol. 1, pp. 329–331. doi: 10.1109/NSWCTC.2010.271
12. Pevny T., Bas P., Fredrich J. Steganalysis by subtractive pixel adjacency matrix. *IEEE Transactions on Information Forensics and Security*, 2010, vol. 5, no. 2, pp. 215–224. doi: 10.1109/TIFS.2010.2045842
13. Shi Y.Q., Xuan G., Yang C., Gao J., Zhang Z., Chai P., Zou D., Chen C., Chen W. Effective steganalysis based on statistical moments of wavelet characteristic function. *Proc. Int. Conf. on Information Technology: Coding and Computing, ITCC'05*. Las Vegas, USA, 2005, vol. 2, pp.

Режим доступа: http://bows2.ec-lille.fr/, свободный. Яз. англ. (дата обращения 12.04.2017).
15. Walia R. Steganography based on neighborhood pixels // Proc. 2nd Conf. on Advances in Computing, Communications and Informatics (ICACCI). Mysore, India, 2013. P. 203–206. doi: 10.1109/ICACCI.2013.6637171
16. Qin J., Xiang X., Deng Y., Li Y., Pan L. Steganalysis of highly undetectable steganography using convolution filtering // Information Technology Journal. 2014. V. 13. N 16. P. 2588–2592. doi: 10.3923/itj.2014.2588.2592

Авторы

Сивачев Алексей Вячеславович – аспирант, Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация, sivachev239@mail.ru

Прохожев Николай Николаевич – кандидат технических наук, доцент, Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация, jesau2@yandex.ru

Михайличенко Ольга Викторовна – кандидат технических наук, доцент, Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация, 19791109@list.ru

Башмаков Даниил Андреевич – аспирант, Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация, basme@list.ru

768–773.
14. *BOWS2 the 10 000 original images*. Available at: http://bows2.ec-lille.fr/ (accessed 12.04.2017).
15. Walia R. Steganography based on neighborhood pixels. *Proc. 2nd Conf. on Advances in Computing, Communications and Informatics, ICACCI*. Mysore, India, 2013, pp. 203–206. doi: 10.1109/ICACCI.2013.6637171
16. Qin J., Xiang X., Deng Y., Li Y., Pan L. Steganalysis of highly undetectable steganography using convolution filtering. *Information Technology Journal*, 2014, vol. 13, no. 16, pp. 2588–2592. doi: 10.3923/itj.2014.2588.2592

Authors

Aleksey V. Sivachev – postgraduate, ITMO University, Saint Petersburg, 197101, Russian Federation, sivachev239@mail.ru

Nikolay N. Prokhozhev – PhD, Associate Professor, ITMO University, Saint Petersburg, 197101, Russian Federation, jesau2@yandex.ru

Olga V. Mikhailichenko – PhD, Associate Professor, ITMO University, Saint Petersburg, 197101, Russian Federation, 19791109@list.ru

Daniil A. Bashmakov – postgraduate, ITMO University, Saint Petersburg, 197101, Russian Federation, basme@list.ru