ЭФФЕКТИВНОСТЬ СТЕГАНОАНАЛИЗА НА ОСНОВЕ МЕТОДОВ МАШИННОГО ОБУЧЕНИЯ

Сивачев А.В.[1], Прохожев Н.Н.[2], Михайличенко О.В.[3], Башмаков Д.А.[4]

Предметом исследования данной работы является точность современных методов стеганоанализа на основе машинного обучения. Исследуемые методы являются наиболее перспективными в задачах пассивного противодействия стеганографическим каналам передачи информации, организуемым на основе сокрытия в область дискретного вейвлет–преобразования (ДВП) неподвижных цифровых изображений. Проведенный в работе сравнительный анализ позволяет не только оценить практические возможности стеганоанализа на основе современных методов, но и упростить выбор конкретного метода и параметров машинного обучения при построении системы стеганоанализа. В основе исследования лежит принцип создания равных условий для всех исследуемых методов стеганоанализа. Стеганографическое воздействие моделируется путем изменения значений младших значащих бит коэффициентов ДВП всех областей по отдельности, получаемых при одноуровневом разложении изображения. Тестовое и обучающее множества изображений содержат значительное количество элементов. Полезная нагрузка стеганоизображения имеет фиксированные и одинаковы для всех исследуемых методов значения. Основными результатами проведенного исследования являются графики и таблицы, отображающие точность классификации современных методов стеганоанализа на основе машинного обучения. Результаты приведены для всех четырех плоскостей коэффициентов ДВП и различных значений величины полезной нагрузки, как при обучении, так и при распознавании стеганоизображения. Результаты позволяют оценить не только возможности современных методов по точности детектирования факта встраивания скрытой информации в область коэффициентов ДВП, но и максимальную пропускную способность стеганоканала в условиях пассивного противодействия.

***Ключевые слова**: стеганография, пассивное противодействие, стеганоканал, скрытый канал передачи, система и алгоритмы стеганоанализа, бинарная классификация, низкочастотная область одномерного ДВП, дискретное вейвлет–преобразование, преобразование Хаара и Добеши, принцип создания равных условий .*

DOI: 10.21681/2311-3456-2017-2-53-60

Введение

В современном глобальном информационном пространстве стеганография может быть успешно использована в задачах организации скрытых каналов передачи информации [1, 2]. Применение стеганографии для создания скрытых каналов передачи информации все чаще встречается как в деятельности 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 информации [5].

В целях пассивного противодействия стеганографическим каналам на основе дискретного вейвлет-преобразования (ДВП) встраивания разрабатываются методы стеганоанализа, позволяющие определить факт стеганографического воздействия на цифровое изображение. 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 стеганографического воздействия [6, 7]. В тоже 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 [8]. Перспективным направлением стеганоанализа для области ДВП является использование методов на основе машинного обучения.

1 Сивачев Алексей Вячеславович, Университет ИТМО, Санкт-Петербург, Россия, sivachev239@mail.ru
2 Прохожев Николай Николаевич, кандидат технических наук, Университет ИТМО, Санкт-Петербург, Россия, jesau2@yandex.ru
3 Михайличенко Ольга Викторовна, кандидат технических наук, Университет ИТМО, Санкт-Петербург, Россия, 19791109@list.ru
4 Башмаков Даниил Андреевич, Университет ИТМО, Санкт-Петербург, Россия, basme@list.ru

При практическом решении задачи пассивного противодействия стеганографическим каналам 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, т.к. 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 различных методов стеганоанализа, основываясь на заявленных самими авторами данных, достаточно сложно, т.к. разные авторы используют разные коллекции изображений и различные способы моделирования стеганографического воздействия для оценки точности своих алгоритмов. 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.

Цель работы

В работе проводится сравнительная оценка точности рассматриваемых методов стеганоанализа, на основе которой можно выбрать оптимальный метод для пассивного противодействия стеганографическим каналам в различных областях коэффициентов ДВП цифровых изображений.

Методика проведения экспериментов

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

Условия проведения экспериментов

Из современных методов стеганоанализа на основе машинного обучения для исследования были выбраны методы, широко известные и наиболее часто цитируемые:

– алгоритм, предложенный Gireesh Kumar и другими [9];

– алгоритм, предложенный Hany Farid [10];

– алгоритм, предложенный Changxin Liu и другими [11];

– алгоритм SPAM [12];

– алгоритм, предложенный Yun Q. Shi и другими [13].

Для проведения экспериментов были выбраны следующие коллекции изображений:

– коллекция 1 (BOWS2) – 10000 изображений, разрешение 512x512;

– коллекция 2 – 3500 изображений, разрешение 640x480.

Для моделирования стеганографического воздействия применялось одноуровневое ДВП. Встраивание информации моделировалось путем изменения значений младших бит коэффициентов каждой из четырех областей ДВП (LL, LH, HL, HH).

Для формирования обучающей выборки из коллекции 1 и 2 использовалось 20% изображений. Остальные 80% изображений коллекций использовались в качестве тестовой выборки. В каждой выборке количество оригинальных изображений и стеганоизображений было равным.

Способ оценки эффективности методов стеганоанализа

Эффективность метода 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 и FN, где по оси Y располагается количество изображений в процентах, классифицированных соответствующим образом от общего количества.

Результаты исследования

Для наглядного сравнения рассматриваемых в работе методов стеганоанализа, результаты классификации при обучении на стеганоизображениях с 5% полезной нагрузкой, представлены в виде графиков значений TN, TP, FP, FN на (рис. 1–4). 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.

Основные результаты экспериментов, при различных значениях полезной нагрузки в обучающем и тестовом множествах изображений для различных областей встраивания, предоставлены в (табл. 1–4).

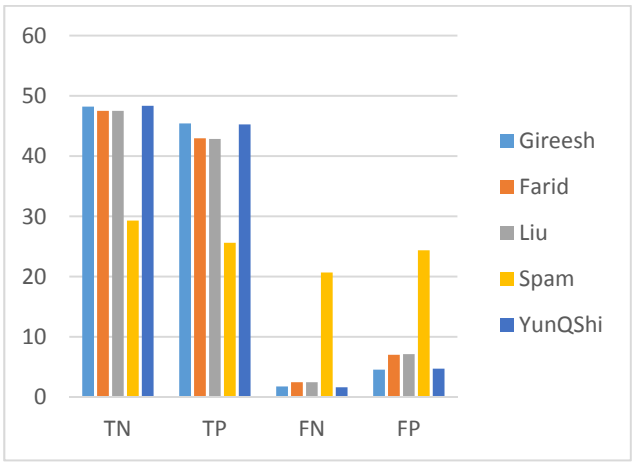


***Рис. 1**. График соотношения TN, TP, FP, FN при встраивании в HH область*

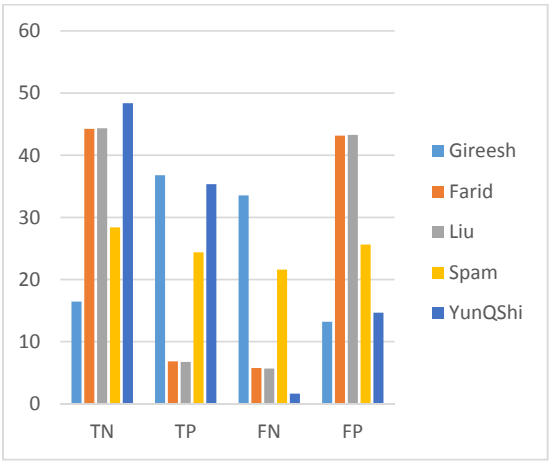


***Рис. 2**. График соотношения TN, TP, FP, FN при встраивании в LH область*

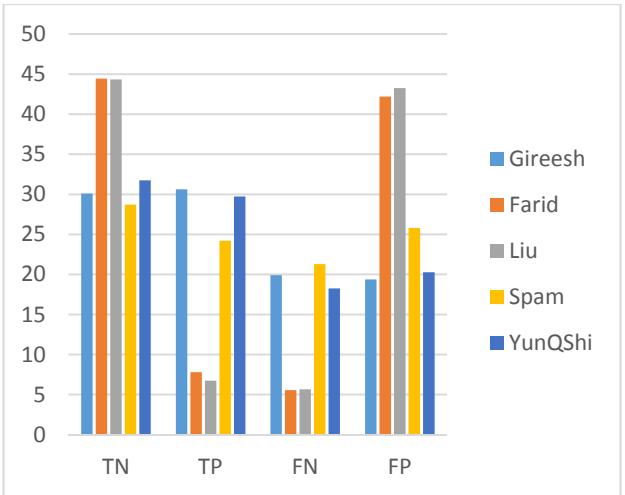


***Рис. 3.** График соотношения TN, TP, FP, FN при встраивании в HL область*

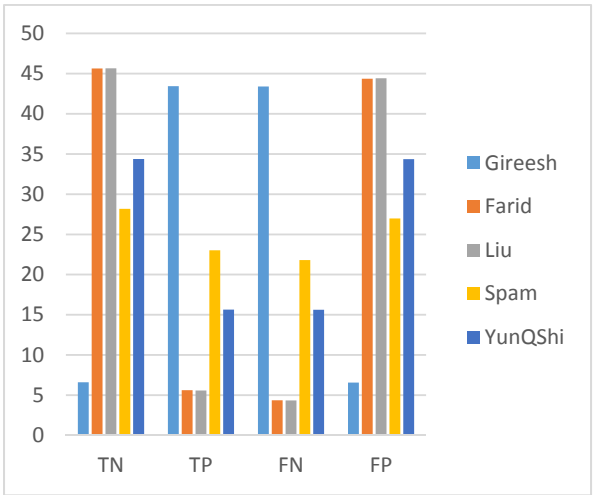


***Рис. 4.** График соотношения TN, TP, FP, FN при встраивании в LL область*

Таблица 1.
Процент верно классифицированных изображений при встраивании в HH область коэффициентов ДВП

Алгоритм	% полезной нагрузки при обучении	% верно классифицированных изображений					
		% полезной нагрузки при оценке					
		0%	1%	5%	10%	15%	20%
Gireesh Kumar	1%	79,32	70,60	96,68	99,05	99,52	99,78
	5%	96,46	11,16	90,88	97,43	99,01	99,49
	10%	97,96	4,25	85,18	96,53	98,44	99,28
	20%	98,72	2,26	78,78	95,38	98,05	99,06
Hany Farid	1%	90,55	17,82	85,82	96,83	98,66	99,33
	5%	95,05	11,9	85,93	96,7	98,54	99,31
	10%	97,08	6,33	82,98	96,13	98,29	99,23
	20%	97,90	4,07	78,80	95,50	98,012	99,06
Chang xin Liu	1%	90,58	17,41	85,63	96,78	98,66	99,33
	5%	95,05	11,89	85,74	96,63	98,53	99,3
	10%	97,06	6,23	82,89	96,06	98,29	99,2
	20%	97,92	4,10	78,66	95,48	97,98	98,98
SPAM	1%	53,35	48,6	56,01	66,91	75,92	80,9
	5%	58,61	43,41	51,23	61,99	72,01	78,51
	10%	64,56	37,18	44,88	55,14	66,88	74,98
	20%	73,96	27,40	33,95	44,05	55,78	67,62
Yun Q. Shi	1%	80,17	70,32	96,57	99,02	99,51	99,77
	5%	96,73	10,74	90,55	97,38	98,94	99,44
	10%	98,23	3,78	84,35	96,36	98,33	99,2
	20%	98,85	1,93	77,18	94,91	97,88	98,98

Таблица 2.
Процент верно классифицированных изображений при встраивании в LH область коэффициентов ДВП

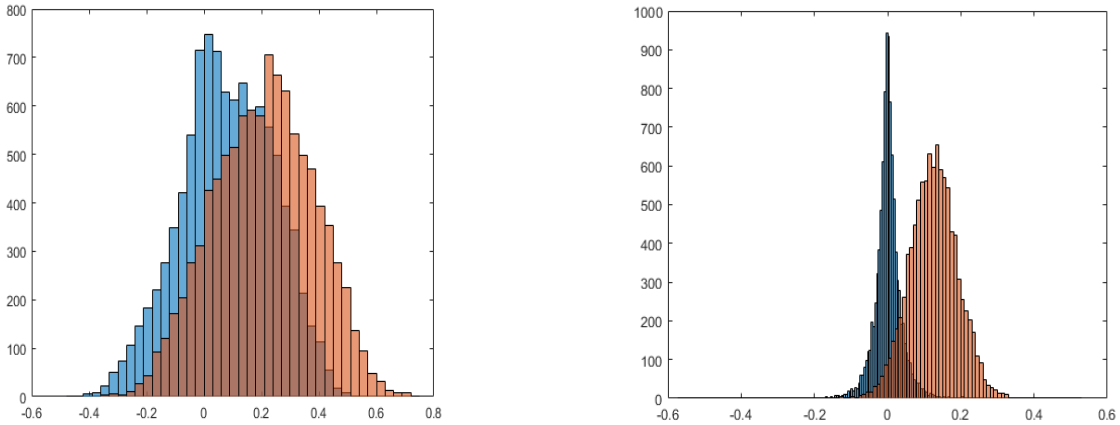
Алгоритм	% полезной нагрузки при обучении	% верно классифицированных изображений					
		% полезной нагрузки при оценке					
		0%	1%	5%	10%	15%	20%
Gireesh Kumar	1%	29,07	72,26	76,91	81,62	85,45	88,31
	5%	32,92	68,47	73,57	78,87	83,12	86,47
	10%	37,92	63,52	69,30	74,82	79,73	83,63
	20%	46,76	54,58	59,90	67,22	72,75	77,67
Hany Farid	1%	90,67	10,45	10,17	9,70	9,31	9,22
	5%	88,48	13,32	13,67	13,77	13,88	14,12
	10%	76,56	24,78	30,45	34,2	38,16	42,15
	20%	23,81	76,88	81,64	86,56	88,85	90,9
Chang xin Liu	1%	90,77	10,41	10,12	9,67	9,26	9,10
	5%	88,66	13,06	13,46	13,53	13,67	13,76
	10%	77,51	23,64	29,05	32,36	36,45	40,4
	20%	25,03	75,69	80,74	85,79	88,44	90,34
SPAM	1%	53,56	47,45	51,87	57,46	63,77	69,53
	5%	56,80	44,31	48,73	54,21	60,41	66,88
	10%	60,21	40,9	45,08	50,5	56,64	63,59
	20%	66,63	34,18	38,3	43,81	49,55	56,2
Yun Q. Shi	1%	80,17	68,01	74,08	79,28	83,15	86,41
	5%	96,72	64,57	70,67	76,55	80,75	84,06
	10%	98,22	60,08	65,71	72,69	77,64	81,53
	20%	98,85	51,48	56,84	64,19	70,61	75,49

Таблица 3.
Процент верно классифицированных изображений при встраивании в HL область коэффициентов ДВП

Алгоритм	% полезной нагрузки при обучении	% верно классифицированных изображений					
		% полезной нагрузки при оценке					
		0%	1%	5%	10%	15%	20%
Gireesh Kumar	1%	49,28	55,32	69,93	81,25	87,63	91,66
	5%	60,19	44,15	61,24	75,26	83,9	88,85
	10%	71,36	31,86	49,13	66,91	77,98	84,91
	20%	84,38	17,43	29,3	49,56	65,6	75,6
Hany Farid	1%	90,92	10,37	10,17	9,83	9,83	10,00
	5%	88,88	13,34	15,61	19,11	23,53	29,58
	10%	76,93	25,33	39,1	54,83	67,7	76,1
	20%	61,86	42,03	58,14	73,75	81,65	86,66
Chang xin Liu	1%	91,01	10,32	10,11	9,76	9,68	9,87
	5%	89,04	13,16	15,13	18,71	22,79	28,83
	10%	77,39	24,6	38,6	53,98	67,45	75,86
	20%	62,08	41,8	57,64	73,79	81,71	86,8
SPAM	1%	54,22	46,92	51,52	57,60	64,22	70,33
	5%	57,41	43,73	48,4	54,13	61	67,9
	10%	61,26	39,68	44,36	50,26	56,89	64,44
	20%	68,11	32,74	36,95	42,94	49,5	56,76
Yun Q. Shi	1%	52,7	52,63	68,36	80,20	86,83	90,92
	5%	63,47	40,80	59,43	73,90	82,68	87,93
	10%	73,77	29,38	47,03	65,63	76,70	83,60
	20%	85,63	16,06	26,91	47,65	63,81	74,11

Таблица 4
Процент правильно классифицированных изображений для встраивания в LL область коэффициентов ДВП

Алгоритм	% полезной нагрузки при обучении	% верно классифицированных изображений					
		% полезной нагрузки при оценке					
		0%	1%	5%	10%	15%	20%
Gireesh Kumar	1%	12,97	87,05	87,11	87,25	87,32	87,38
	5%	13,21	86,83	86,88	87,03	87,12	87,21
	10%	13,00	87,06	87,16	87,30	87,42	87,57
	20%	13,48	86,55	86,61	86,68	86,77	86,93
Hany Farid	1%	91,76	10,08	8,75	7,15	5,86	5,05
	5%	91,26	11,43	11,25	9,83	8,47	7,52
	10%	52,45	48,58	54,92	62,72	67,01	70,13
	20%	18,40	82,16	85,56	89,28	91,93	93,66
Chang xin Liu	1%	91,85	10,06	8,67	7,07	5,86	4,96
	5%	91,33	11,30	11,13	9,72	8,27	7,41
	10%	55,92	45,10	50,76	58,41	63,12	66,27
	20%	19,22	81,45	85,02	88,91	91,83	93,57
SPAM	1%	55,21	45,27	47,03	49,57	51,83	54,36
	5%	56,37	44,17	46,02	48,30	50,58	53,07
	10%	57,47	42,91	44,85	47,06	49,40	51,70
	20%	59,81	40,51	42,47	44,76	47,15	49,28
Yun Q. Shi	1%	71,80	28,20	28,23	28,25	28,35	28,23
	5%	68,75	31,31	31,30	31,13	31,46	31,41
	10%	71,83	28,28	28,18	28,22	28,15	28,47
	20%	60,52	39,48	39,62	39,47	39,60	39,68



а) *б)*

***Рис. 5**. Гистограмма значений первого статистического момента для HL области оригинальных (синий) и стегано- (оранжевый) изображений при использовании вейвлет преобразований а) Хаара, б) Добеши*

Выводы

Современные методы стеганоанализа на основе методов машинного обучения позволяют детектировать стеганоизображение со встраиванием в НН область коэффициентов ДВП при полезной нагрузке пять и более процентов. Наиболее высокую эффективность «по совокупности» процента верно классифицированных оригинальных и стеганоизображений для НН области показали алгоритмы, предложенные в [9,13].

Точность детектирования современных методов стеганоанализа для LH и HL областей коэффициентов ДВП значительно уступает аналогичному параметру для области НН, что не позволяет организовать эффективное пассивное противодействие стеганографическим каналам с полезной нагрузкой менее 15-20%.

Результаты, полученные для LL области коэффициентов ДВП, отражают практическую невозможность детектирования факта встраивания скрытой информации. При этом стоит отметить, что изменения, вносимые при стеганографическом воздействии 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 стегано- изображений пересекаются (рис. 5 (а)) что, как следствие, затрудняет классификацию изображения по данным параметрам. Аналогичные исследования, проведенные для вейвлет-преобразования Добеши, демонстрируют перспективную картину (рис. 5 (б)) относительно возможности машинного обучения.

Одним из недостатков рассматриваемых алгоритмов является игнорирование известных зависимостей между значениями коэффициентов различных областей вейвлет-преобразования. На (рис.6) приведен график зависимости первого статистического момента для HL области двумерного вейвлет-преобразования (рис.5 (а)) от статистического момента, полученного с использованием низкочастотной области одномерного вейвлет-преобразования для оригинального изображения.

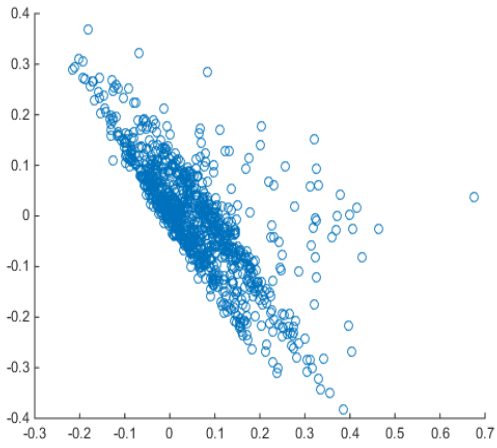


***Рис. 6**. График зависимости первого статистического момента для HL области от статистического момента, полученного с использованием низкочастотной области одномерного вейвлет-преобразования*

При стеганографическом воздействии на коэффициенты 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 стеганографическим воздействием на область HL двумерного вейвлет-преобразования, и упростить задачу классификации.

Заключение

Встраивание информации в область ДВП изображения на данный момент имеет потенциал в задачах организации стеганоканала, т.к. современные методы стеганоанализа не в состоянии оказать эффективное противодействие в отношении стеганоканала, использующего LH и HL области коэффициентов ДВП. Так при одноуровневом разложении для изображения размером 512x512 пикселей получается четыре области коэффициентов: LL, LH, HL и HH. Каждая область ДВП имеет размер 256x256 коэффициентов. В LH и HL области коэффициентов ДВП 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. Таким образом, необходимо дальнейшее совершенствование методов стеганоанализа для обнаружения факта встраивания в область ДВП 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 стегоизображений.
2. Поиск и использование дополнительных параметров изображения для формирования опорных векторов, позволяющих повысить однозначность разделения множества оригинальных изображений и стегоизображений.

***Рецензент**: Коробейников Анатолий Григорьевич, доктор технических наук, профессор Университета ИТМО, Санк-Петербург, korobeynikov_a_g@mail.ru*

Литература:

1. Грибунин В.Г. и др. Цифровая стеганография. М.: СОЛОН-Пресс, 2002. 272 с.
2. Конахович Г.Ф., Пузыренко А.Ю. Компьютерная стеганография. Теория и практика. К.: МК-Пресс, 2006. 288 с.
3. Steganography: A Powerful Tool for Terrorists and Corporate Spies [Электронный ресурс]: Stratfor - Режим доступа: https://www.stratfor.com/analysis/steganography-powerful-tool-terrorists-and-corporate-spies.
4. An Overview of Steganography for the Computer Forensics Examiner [Электронный ресурс]: Forensic Science Communications - July 2004 Режим доступа: https://www.fbi.gov/about-us/lab/forensic-science-communications/fsc/july2004/research / 2004_03_research01.htm.
5. C. Gayathri, V. Kalpana Study on image steganography techniques [Текст], International Journal of Engineering and Technology (IJET) 2013 Vol. 5 Pages 572-577.
6. Prokhozhev N., Mikhailichenko O., Sivachev A., Bashmakov D., Korobeynikov A.G. Passive Steganalysis Evaluation: Reliabilities of Modern Quantitative Steganalysis Algorithms [Текст], Advances in Intelligent Systems and Computing. 2016. Vol. 451. pp. 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. A. Nissar, A.H.Mir Classification of steganalysis techniques: A study [Текст], Digital Signal Processing, 2010 vol.20 pp. 1758–1770.
9. Gireesh Kumar T., Jithin R., Deepa D. Shankar Feature Based Steganalysis Using Wavelet Decomposition and Magnitude Statistics [Текст], Advances in Computer Engineering (ACE), 2010, pp. 298-300.
10. Farid Hany Detecting Steganographic Messages in Digital Images [Текст], Technical Report TR2001-412, Dartmouth College, Computer Science Department, 2001.
11. Changxin Liu, Chunjuan Ouyang, Ming Guo, Huijuan Chen Image Steganalysis Based on Spatial Domain and DWT Domain Features [Текст], Proceedings of the 2010 Second International Conference on Networks Security, Wireless Communications and Trusted Computing - Volume 01, pp. 329-331.
12. T.Pevny, P.Bas, J.Fredrich Steganalysis by subtractive pixel adjacency matrix [Текст], Transactions on Information Forensics and Security, Volume 5 Issue 2, June 2010 pp. 215-224.
13. Y. Q. Shi, Guorong Xuan, Chengyun Yang, Jianjiong Gao, Zhenping Zhang, Peiqi Chai, Dekun Zou, Chunhua Chen, Wen Chen Effective steganalysis based on statistical moments of wavelet characteristic function [Текст], International Conference on Information Technology: Coding and Computing (ITCC›05) - Volume II 2005, p 768-773.

EFFICIENCY OF STEGANALYSIS BASED ON MACHINE-LEARNING METHODS

Sivachev A.M.[5], Prokhozhev N.N.[6], Mikhailichenko O.V.[7], Bashmakov D. A.[8]

The subject–matter of this work is accuracy of the modern methods of steganalysis based on machine–learning methods. The research methods have the most potential in passive countermeasures against steg–anographic channels of information transmission that are based on hiding static digital images in the area of discrete wavelet decomposition (DWD). The comparative analysis not only assesses the practical capabilities of steganalysis based on modern approaches and simplifies the selection of a specific method and machine learning parameters when building the system of steganalysis. The research is based on the principle of creating equal conditions for all steganalysis methods being studied. A steganographic impact is modelled by changing the values of the least significant bits of DWD indices in each individual area obtained by single–level image decomposition. The test and learning sets of images contain a significant number of elements. The active load of the steganoimage has registered values that are similar for all the study methods. The main results of the study are diagrams and tables which reflect the accuracy of classification of modern methods of steganalysis based on machine–learning methods. The results are specified for all four planes of DWD indices and various values of the active load, both for learning and recognition of steganoimage. The results allow assessing the modern methods for accuracy of detecting hidden information embedded in the DWD indices area, and maximum capacity of steganochannel in the conditions of passive countermeasures.

Keywords*: steganography, passive attack, hiding channels, machine learning, 1–level high frequency planes DWT, system and algorithms of steganalisys, binary classification, Haar and Daubechies transform*

References:

1. Gribunin V.G. Tsifrovaya steganografiya [Tekst]: monografiya. M.: SOLON-Press, 2002. 272 P.
2. Konakhovich G.F., Puzyrenko A.Yu. Komp›yuternaya steganografiya. Teoriya i praktika. K.: MK-Press, 2006. 288 P.
3. Steganography: A Powerful Tool for Terrorists and Corporate Spies [Elektronnyy resurs]: Stratfor - Rezhim dostupa: https://www.stratfor.com/analysis/steganography-powerful-tool-terrorists-and-corporate-spies.
4. An Overview of Steganography for the Computer Forensics Examiner [Elektronnyy resurs]: Forensic Science Communications - July 2004 Rezhim dostupa: https://www.fbi.gov/about-us/lab/forensic-science-communications/fsc/july2004/research / 2004_03_research01.htm.
5. C. Gayathri, V. Kalpana Study on image steganography techniques [Tekst], International Journal of Engineering and Technology (IJET) 2013 Vol. 5 Pages 572-577.
6. Prokhozhev N., Mikhailichenko O., Sivachev A., Bashmakov D., Korobeynikov A.G. Passive Steganalysis Evaluation: Reliabilities of Modern Quantitative Steganalysis Algorithms [Tekst], 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., Mikhaylichenko O.V., Bashmakov D.A., Sivachev A.V., Korobeynikov A.G. Issledovanie effektivnosti primeneniya statisticheskikh algoritmov kolichestvennogo steganoanaliza v zadache detektirovaniya skrytykh kanalov peredachi informatsii, Programmnye sistemy i vychislitel›nye metody. 2015. No 3, pp. 281-292. DOI: 10.7256/2305-6061.2015.3.17233.
8. A. Nissar, A.H.Mir Classification of steganalysis techniques: A study [Tekst], Digital Signal Processing, 2010 vol.20 pp. 1758–1770.
9. Gireesh Kumar T., Jithin R., Deepa D. Shankar Feature Based Steganalysis Using Wavelet Decomposition and Magnitude Statistics [Tekst], Advances in Computer Engineering (ACE), 2010, pp. 298-300.
10. Farid Hany Detecting Steganographic Messages in Digital Images [Tekst], Technical Report TR2001-412, Dartmouth College, Computer Science Department, 2001.
11. Changxin Liu, Chunjuan Ouyang, Ming Guo, Huijuan Chen Image Steganalysis Based on Spatial Domain and DWT Domain Features [Tekst], Proceedings of the 2010 Second International Conference on Networks Security, Wireless Communications and Trusted Computing - Volume 01, pp. 329-331.
12. T.Pevny, P.Bas, J.Fredrich Steganalysis by subtractive pixel adjacency matrix [Tekst], Transactions on Information Forensics and Security, Volume 5 Issue 2, June 2010 pp. 215-224.
13. Y. Q. Shi, Guorong Xuan, Chengyun Yang, Jianjiong Gao, Zhenping Zhang, Peiqi Chai, Dekun Zou, Chunhua Chen, Wen Chen Effective steganalysis based on statistical moments of wavelet characteristic function [Tekst], International Conference on Information Technology: Coding and Computing (ITCC›05) - Volume II 2005, p 768-773.

5 Aleksei Sivachev, St. Petersburg National Research University of Information Technologies, Mechanics and Optics, St. Petersburg, sivachev239@mail.ru

6 Nikolai Prokhozhev, Ph.D., St. Petersburg National Research University of Information Technologies, Mechanics and Optics, St. Petersburg, jesau2@yandex.ru

7 Olga Mikhailichenko, Ph.D., St. Petersburg National Research University of Information Technologies, Mechanics and Optics, St. Petersburg, 19791109 @list.ru

8 Daniil Bashmakov, St. Petersburg National Research University of Information Technologies, Mechanics and Optics, St. Petersburg, basme@list.ru