Математические структуры и моделирование
2020. № 4(56). С. 75–102

УДК 004.932.2
DOI 10.24147/2222-8772.2020.4.75-102

ОБЗОР МЕТОДОВ СТЕГАНОГРАФИЧЕСКОГО АНАЛИЗА ИЗОБРАЖЕНИЙ В РАБОТАХ ЗАРУБЕЖНЫХ АВТОРОВ

Д.Э. Вильховский
ассистент кафедры информационной безопасности, e-mail: vilkhovskiy@gmail.com

Омский государственный университет им. Ф.М. Достоевского, Омск, Россия

Аннотация. В статье представлен обзор зарубежных исследований в области стеганографического анализа изображений, направленного на обнаружение стеговставок, выполненных на основе алгоритмов замены наименее значащих битов и дискретного косинусного преобразования. Отмечается, что дальнейшее развитие методологии стегоанализа идёт в двух направлениях: уменьшение трудоёмкости и стоимости вычислений при сохранении высокого уровня чувствительности, что вполне оправдывает себя в случае наличия стеговставок с достаточно большой полезной нагрузкой, т. е. при полном заполнении стегоконтейнера, или повышение эффективности методов распознавания изображений со стеговставками при условии низкого уровня заполнения стегоконтейнера. При этом в последние пять лет доминирующую роль в стеганографическом анализе стали занимать методы, основанные на машинном и глубоком обучении.

Ключевые слова: стегоанализ, стеганографический анализ, LSB-вставка, метод замены наименее значащих битов.

Введение

Если стеганография имеет целью незаметную передачу данных, встроенных в какое-либо мультимедиа так, чтобы сам факт встраивания оставался незамеченным, то стеганографический анализ (стегоанализ) направлен на обнаружение встроенных данных, т. е. факта встраивания. Соответственно, являясь антагонистическими по своей сущности, оба направления находятся в непрерывном развитии. В первом случае речь идёт о разработке новых методов, алгоритмов и схем встраивания, а во втором — о разработке методов, моделей и алгоритмов обнаружения встраивания.

В большинстве случаев разрабатываются универсальные (слепые) методы стегоанализа, призванные эффективно работать при любых алгоритмах и схемах встраивания в условиях слепого применения, т. е. когда алгоритмы и схемы встраивания неизвестны стегоаналитику. Единственным допущением, закладывающимся при разработке универсальных методов, является допущение о методе встраивания, что важно для определения того, в какой области (пространственной или преобразования) осуществляется встраивание.

В данной статье исследуются методы стегоанализа, работающие на обнаружение встраиваний в пространственную область, выполненных путём замены наименее значащих битов.

Статья содержит ряд специфических терминов, пришедших из англоязычных исследований. Для удобства прочтения и понимания представленного материала в таблице 1 приводится перечень основных терминов с расшифровкой их аббревиатуры на английском языке и значения на русском.

Таблица 1. Перечень терминов, используемых в настоящей статье

Термин	Расшифровка на английском языке	Значение на русском языке
ALE	Amplitude of local extrema	Амплитуда локальных экстремумов
ANOVA	ANalysis Of VAriance	Дисперсионный анализ
CNN	Convolutional neural network	Свёрточная нейронная сеть
CSW	Channel similarity weight	Вес подобий цветовых каналов
DCT	Discrete Cosine Transform	Дискретное косинусное преобразование
FAR	False Alarm Rate	Частота ложных тревог
FDR	False Detection Rate	Частота ложных обнаружений
FLD	Fisher Linear Discriminant	Линейный дискриминант Фишера
GLCM	Gray Level Co-occurrence Matrix	Матрица совпадений уровней серого
HCF	Histogram characteristic function	Характеристическая функция гистограммы
HCF-COM	Histogram characteristic function — center of mass	Характеристическая функция гистограммы с использованием центра масс
LSB	Least Significant Bit	Наименьший значимый бит
PDF	Probability Density Function	Функциия плотности вероятности
PoV	Pairs of Values	Пары значений
PSO	Particle Swarm Optimization	Оптимизация роя частиц
PSW	Pixel Similarity Weight	Вес подобий пикселей
QMF	Quadrature Mirror Filter	Квадратурный зеркальный фильтр
RBF	Radial Basis Function	Радиальная базисная функция
RHB	Right Half-Byte	Правый полубайт
RS	Regular or Singular	Регулярный или сингулярный
SC	Simplicial Complex	Симплициальный комплекс
SC Rips	Vietoris-Rips complex	Симплициальный комплекс Виеториса–Рипса
SRM	Spatial Rich Model	Пространственнобогатая модель
SVM	Support Vector Machine	Метод опорных векторов
SW	Similarity Weight	Вес подобий
T	Threshold	Порог (пороговые значения)

Продолжение таблицы 1

Термин	Расшифровка на английском языке	Значение на русском языке
TDA	Topological Data Analysis	Анализ топологических данных
ULBP	Uniform Local Binary Pattern	Однородный локальный двоичный шаблон
WAM	Wavelet Absolute Moments	Абсолютные вейвлет-моменты

1. Обзор ранних исследований в области обнаружения LSB-вставок

В последние годы прошлого столетия как ответ на развитие методов стеганографии появились первые работы в области стеганографического анализа. В течение последующих лет отмечено возрастание интереса к проблемам обнаружения стеганографических вставок, что находит отражение в ежегодном увеличении количества работ данной проблематики.

В таблице 2 представлен перечень наиболее значимых работ, посвящённых стеганографическому анализу и опубликованных в ранний период. Представленные работы можно охарактеризовать как основополагающие, поскольку именно в них были впервые предложены различные методы слепого (универсального) стегоанализа, определившие вектор дальнейших изучений в этой области.

Таблица 2. Методы стеганографического анализа в ранних работах

Авторы	Год издания	Краткое описание предложенного метода
Метод Хи-квадрата		
Westfeld A. et al, [35–37]	1999 – 2002	Использует статистический анализе пар значений (PoV), которыми обмениваются во время встраивания секретных данных. Основан на том, что любые стеганографические методы изменяют частоту пары значений в процессе встраивания сообщения
RS-стегоанализ		
Fridrich J. et al. [12–14]	2000 – 2003	Впервые предложен метод регулярного и сингулярного анализа (RS-стегоанализа). В качестве отличительного признака используются близкие цветовые пары в 24-битных цветных изображениях и классификации пикселей на обычные и особые группы. Частота этих групп определяет длину секретного сообщения в стего-изображениях
Gul G. et al [17]	2010	Основан на линейных зависимостях строк / столбцов изображений в локальных окрестностях с использованием разложения по сингулярным значениям

Продолжение таблицы 2

Авторы	Год издания	Краткое описание предложенного метода
Анализ на основе вейвлет-разложения и статистики		
Farid H. et al [26]	2002	Впервые для построения статистических моделей высокого порядка естественных изображений используются вейвлет-разложения. Для различения нетронутых и искаженных изображений используется линейный дискриминантный анализ Фишера
Lyu S. et al [27]	2004	Учитывает зависимости между цветовыми каналами. Использует моменты остаточного шума более высокого порядка, полученные с использованием предикторов коэффициентов в QMF-разложении изображения из всех трёх цветовых каналов
Анализ на основе гистограмм		
Harmsen J., Pearlman W [18]	2003	Модель, известная как HCF-COM. Построена с использованием модели аддитивного шума. Основана на использовании центра тяжести характеристической функции гистограммы (HCF) с калибровкой путём повторной выборки и суммирования цветовых компонентов
Ker et al. [20–22]	2004 – 2005	Улучшены характеристики обнаружения метода стегоанализа HCF-COM, в модель HCF-COM добавлен механизм калибровки и гистограммы смежности
Zhang J. et al. [44], Cancelli G. et al. [2]	2007 – 2008	Модель, известная как ALE-модель. Основана на вычислении из гистограммы изображений амплитуды локальных экстремумов (ALE). В качестве стегоаналитического признака вычисляется сумма абсолютной разницы в значениях между локальными экстремумами и соседями гистограммы
Методы на основе машинного обучения		
Dumitrescu S. et al [9]	2005	Разработан как для цветных изображений, так и для изображений в градациях серого. Использует статистику более высокого порядка для вывода уравнений обнаружения и определения длины сообщения
Goljan M et al [15]	2006	Использует в качестве признаков 27 абсолютных вейвлет моментов (WAM) остаточного шума, полученного из трёх поддиапазонов более высоких частот в области вейвлета. В качестве классификатора используется линейный дискриминант Фишера (FLD)
Dumitrescu S. et al. [8]	2007	Основан на парах отсчётов из сигналов, возникающих в результате LSB-вставок. Как сообщают авторы, является точным, даже при условии малой длины сообщения

Продолжение таблицы 2

Авторы	Год издания	Краткое описание предложенного метода
Pevny T. et al [29]	2010	Для моделирования взаимосвязи между различиями соседних пикселей в восьми направлениях используются марковские процессы первого и второго порядка (с 686 элементами). В качестве классификатора используется метод опорных векторов (SVM)
Пространственнобогатая модель (SRM-модель)		
Fridrich J. et al [19]	2012	Многомодельная комбинированная функция, которая использует линейные и нелинейные вычисления зависимостей между соседними пикселями для количественной оценки шума изображений и матрицу совместной встречаемости высокого порядка в качестве основных характеристик

2. Обзор некоторых методов стеганографического анализа, предложенных в период 2014–2020 гг.

2.1. Ансамблевый SW-стегоанализ с применением машинного обучения

В работах [3, 4] описан низкоразмерный метод ансамблевого стегоанализа LSB-замены изображения с диапазоном встраивания до 0,25 бит на пиксель путём вычисления весов подобий (далее – ансамблевый SW-стегоанализ).

Общая характеристика метода

Метод основан на цветовой корреляции между пикселями и цветовыми каналами трёх различных классах в соседних зонах и гипотезе, что пиксели или каналы одинаковой интенсивности в каждой соседней зоне по-разному влияют на окончательное значение весов их подобий.

Сущность, характеристики и примеры классов пикселей представлены в таблице 3.

Таблица 3. Сущность, характеристики и область расположения классов пикселей

Класс пикселей	Характеристика	Область расположения
Плоский	Имеют самый высокий уровень цветовой корреляции	Область со сплошным цветом

Класс пикселей	Характеристика	Область расположения
Гладкий	Средний уровень цветовой корреляции	Цвет пикселей изменяется постепенно в более широком пространстве
Резкий	Самая низкая цветовая корреляция	Цвет пикселей меняется постоянно и резко

SW-анализ

В качестве аналитических параметров вычисляются веса подобий пикселей (PSW) и цветовых каналов (CSW), создаются наборы данных PSW и CSW, содержащих результаты анализа для каждого пикселя в трёх соседних зонах. Таким образом, для последующего обучения и классификации создаются шесть эталонных профилей со статистическими характеристиками изображений, включающие обнаруженные классы пикселей и степени принадлежности всех пикселей изображения.

В качестве эффективной границы анализа для PSW и CSW экспериментальным и оценочным способами определена третья соседняя зона.

Классификатор

В качестве классификатора используется метод опорных векторов с применением трапециевидной нечёткой функции принадлежности.

Разработанное ядро (SVM-ядро) поддерживает множественное членство и определяет степень членства для каждой согласованной группы данных. Структура разработанного SVM-ядра основывается на таких статистических функциях, как гауссовое (нормальное) распределение, правило трёх сигм и стандартное отклонение от среднего, что позволяет устранять естественный шум данных.

Принятие окончательного решения осуществляется в соответствии с иерархическими решениями, принятыми в подкомпонентах PSW и CSW, а также ансамблевой интерпретации.

Оценка эффективности метода

Для оценки эффективности методов стегоанализа использовались такие метрики, как процент истинно положительных сигналов тревоги от общего количества проанализированных экземпляров (основной критерий) и процент правильно обнаруженных чистых (без стего-вставок) изображений. Данные об эффективности метода представлены в таблице 4.

Таблица 4. Чувствительность PSW, CSW и ансамблевого SW методов, %

	PSW	CSW	Ансамблевый SW
Чистое изображение			
Зона 1	0	0	0
Зона 2	81,315	8,968	8,641

	PSW	CSW	Ансамблевый SW
Зона 3	67,115	91,928	66,8161
Изображение со стеговставкой, коэффициент встраивания 0,125			
Зона 1	100	68,983	100
Зона 2	56,325	68,983	100
Зона 3	74,887	64,573	86,7713
Изображение со стеговставкой, коэффициент встраивания 0,25			
Зона 1	68,983	68,983	100
Зона 2	100	56,875	100
Зона 3	98,056	74,1405	99,626

PSW более эффективен при более высоком уровне заполнения стегоконтейнера, в то время как CSW более эффективен при более низких соотношениях. Таким образом, делается вывод, что для достижения наилучших общих результатов необходимо использовать комбинацию методов интерпретации PSW и CSW.

Согласно значениям PSW (67,115 %) и SW ансамбля (66,8161 %) недостаточно хороши для надежного обнаружения изображения обложки. Следовательно, авторы отмечают, что метод рассчитан на CSW из-за обеспечения надёжной работы с 91,928 % достигнутого успеха.

Данный метод стегоанализа обеспечивает чувствительность 86,77 % при коэффициенте внедрения 0,125 бит на пиксель. При 0,25 бит на пиксель эта чувствительность выросла до 99,626 %, что является логичным следствием большего уровня заполнения стегоконтейнера.

2.2. Стегоанализ на основе статистики текстур изображения

В работе [1] представлен метод слепого стегоанализа с новым набор функций, включающим матрицу совпадений уровней серого (GLCM) и другую статистику текстур изображения. Для экспериментальной работы был выбран формат одноканального изображения в градациях серого для исходных изображений.

Общая характеристика метода

Фокусное внимание предлагаемого метода сосредоточено на свойствах текстуры правого полубайта (RHB) 8-битного канала изображения в градациях серого, представляющего собой область наибольшего встраивания при любом алгоритме встраивания.

Встраивание осуществлялось с использованием схем 2LSB (замена двух бит LSB в байтах изображения) и 4LSB (замена четырёх бит LSB в байтах изображения). При 4LSB-схеме уровень заполнения стегоконтейнера составил около 50 %. При 2LSB-схеме заполнение стегоконтейнера составило 25 %.

Исследуемые признаки

Для анализа используются 22 элемента признаков, для каждого из которых определяется соответствующий вектор признаков как для чистого изображения, так и для стего.

Основными компонентами набора функций являются матрица совпадений уровней серого (GLCM), энтропия правых полубайтов, корреляция между левым и правым полубайтами, коэффициент вариации правых полубайтов и абсолютная разница между последовательными правыми полубайтами, а также дополнительные статистические показатели, которые призваны способствовать различению стего и чистых изображений. В таблице 5 приведён список предлагаемых элементов набора функций.

Таблица 5. Элементы набора характеристик

Характеристика	Описание	Примечание
CC-LR	Коэффициент корреляции между LHB и RHB	Является показателем изменения взимомосвязи между двумя половинами после вложения в правый полубайт
CVR	Коэффициент вариации правых полубайтов	Рассчитывается как отношение стандартного отклонения к среднему, вычисляется для правой половины вертикального среза изображения
GLCM-B	Контраст, корреляция, однородность и энергия полных байтов	Рассчитываются для всего изображения, т. е. для столбца полных байтов
GLCM-R	Контрастность, корреляция, однородность и энергия, RHB	Рассчитываются для правой половины вертикального среза изображения, который состоит из столбца правых полубайтов
GLCM-3	Контрастность, корреляция, однородность и энергия 4LSB	Рассчитываются для вертикальных срезов 3LSB изображения
GLCM-2	Контрастность, корреляция, однородность и энергия, 2LSB	Рассчитываются для вертикальных срезов 2LSB изображения
Энтропия-R	Энтропия RHB	Вычисляется для правой половины вертикального среза изображения

Продолжение таблицы 5

Характеристика	Описание	Примечание
Diff-R	Среднее значение абсолютной разницы между последовательными RHB	Фокусируется на влиянии изменений в правой половине изображения в результате встраивания

Классификатор

В качестве классификатора используется метод опорных векторов (SVM).

Оценка эффективности метода

Результаты классификации чистых изображений и изображений с применением 2LSB и 4LSB стеганографических схем представлены в таблице 6.

Таблица 6. Результаты классификации изображений с 2LSB и 4LSB, %

Оценочные показатели	2LSB	4LSB
Истинно положительный (TP)	99,22	100
Ложно-негативный (FN)	0,78	0
Истинно негативный (TN)	98,82	98,82
Ложно-позитивный (FP)	1,18	1,18
Точность обнаружения	99,02	99,41

Данные свидетельствуют о высокой точности обнаружения чистого и стегоизображения при применении метода. В обеих схемах встраивания коэффициент обнаружения истинно положительных значений немного выше, чем истинно негативный, это указывает на то, что модель лучше обнаруживает стегоизображения, чем чистые изображения.

4LSB-стегоконтейнер имеет немного более высокую точность обнаружения по сравнению с точностью обнаружения 2LSB-стегоконтейнера: 99,41 % при 4LSB-вставке против 99,02 % при 4LSB-вставке. Этот факт объясняется тем, что стегосхема 4LSB содержит вдвое больше встроенных данных. При этом чувствительность метода к обнаружению истинно негативных значений одинакова для обеих схем встраивания.

2.3. Стегоанализ изображений JPEG на основе машинного обучения

В работах [24,31] представлена методология стегоанализа для изображений формата JPEG при 10 % заполнении стегоконтейнера с 10-кратной перекрёстной проверкой.

Общая характеристика метода

Метод применим для четырёх различных типа стеганографии, включая метод замены наименее значащих бит и использование дискретного косинусного преобразования (DCT). Рассматриваются четыре различных вида выборки: линейная, случайная, стратифицированная и автоматическая.

В работе также используется концепция калибровки, которая помогает получить оценку изображения обложки из изображения стего.

Исследуемые признаки

Анализ проводится с использованием признаков первого, второго порядков, признаков расширенного DCT и признаков Маркова. Общее количество признаков составляет 274, включая 165 признаков первого порядка, 28 признаков второго порядка и 81 признак расширенного DCT и признаков Маркова. Подробная информация об извлечённых признаках приведена в таблице 7.

Для всех исследованных ядер и образцов вычисляются векторы производительности с использованием таких метрик производительности, как надёжность, ошибка классификации и каппа.

Таблица 7. Таблица извлечённых признаков

Тип признака	Метод извлечения	Количество признаков
Признаки первого порядка	Двойная гистограмма	99
	Глобальная гистограмма	11
	Индивидуальная гистограмма	55
Признаки второго порядка	Совместная встречаемость	25
	Вариация	1
	Блочность	2
Признаки Маркова		81
	Общее количество	**274**

Классификатор

В качестве классификатора изначально применяется метод опорных векторов (SVM). В дальнейшем используется классификатор, в котором для оптимизации мощности отдельных методов и преодоления их недостатков объединены метод опорных векторов (SVM) и алгоритм оптимизации роя частиц (PSO) — SVM-PSO-классификатор.

В качестве ядер при классификации используются ядро Епанечникова, точечное / линейное ядро DOT, мультиквадратичное, радиальное, ядро ANOVA и полиномиальное ядро.

Оценка эффективности метода

Результаты классификации с использованием SVM- и SVM-PSO-классификаторов представлены в таблицах 8 и 9.

Таблица 8. Результаты классификации с использованием SVM-классификатора

Ядро	Линейная выборка	Случайная выборка	Стратифицированная выборка	Автоматическая выборка
Dot	8,49	43,27	44,52	44,52
Радиальное	6,12	13,37	11,5	11,5
Полиномиальное	9,11	42,64	43,21	43,21
Мультиквадратичное	10	48,12	49,94	49,94
Епанечникова	6,88	21,32	19,54	19,54
ANOVA	6,58	29,96	30,53	30,53

Таблица 9. Результаты классификации с использованием SVM-PSO-классификатора

Ядро	Линейная выборка	Случайная выборка	Стратифицированная выборка	Автоматическая выборка
Dot	25,54	48,96	49,94	49,94
Радиальное	20,64	26,68	25,22	25,22
Полиномиальное	48,87	49,55	50,36	50,36
Мультиквадратичное	71,5	50,92	51,07	51,07
Епанечникова	11,25	19,18	20,13	20,13
ANOVA	11,4	44,73	42,76	42,76

На основании представленных данных можно сделать вывод, что более низкие результаты сопоставления LSB были получены для линейной выборки с существенным повышением эффективности для остальных типах выборки.

При этом стратифицированная выборка даёт лучшие показатели по сравнению со случайной выборкой практически по всех ядрам, хотя различие не слишком существенное. Однако для ядер Епанечникова и радиального ядра наблюдается снижение результативности. Кроме того, показатели для стратифицированной и автоматической выборок являются идентичными для всех ядер.

Также отмечается, что радиальное ядро показало низкую результативность при всех типах выборок и, таким образом, не подходит для замены LSB. Мультиквадратичное ядро обеспечивает лучшую производительность, хорошие результаты были достигнуты также с полиномиальным и точечным ядрами.

Эффективность метода значительно повышается при использовании SVM-PSO-классификатора для всех ядер и выборок. При этом, если верить представленным данным в линейной выборке, наблюдается увеличение результативности в 5 и 7 раз при использовании полиномиального и мультиквадратичного ядер соответственно.

2.4. Компактный метод с применением машинного обучения

В работе [19] предложен компактный метод стегоанализа изображений с применением машинного обучения для обнаружения изображений с LSB-вставками методом сопоставления для изображений в оттенках серого.

Общая характеристика метода

Метод является низкоразмерным (компактным) и использует малое количество характеристик, позволяющих, тем не менее, эффективно различать чистые изображения и изображения с встроенным сообщением.

Исследуются четыре различных уровня заполнения стегоконтейнера — 100 %, 75 %, 50 % и 25 %.

Компактность схемы обеспечивает низкую компьютерную сложность как на этапе обучения, так и на этапе тестирования.

Исследуемые признаки

Анализ статистического артефакта, возникающего в результате встраивания, осуществляется с использованием 12 характеристик на основе функции плотности вероятности (PDF) разницы соседних пикселей и матрицы совпадения изображений, которые могут отличать стегоизображения от естественных изображений. Извлекаемые характеристики представлены в таблице 10.

Оценка эффективности метода

Таблица 10. Извлекаемые характеристики

Тип	Количество	Состав
Характеристики, связанные с параметром формы PDF и разницы значений соседних пикселей при 4 и 8 смежности	2	1. Соотношение параметра формы PDF разности соседних пикселей при 4-связной смежности между входным изображением и стегоизображением 2. Отношение параметра формы PDF к разности соседних пикселей при 8-связной смежности между входным изображением и стегоизображением

Продолжение таблицы 10

Тип	Количество	Состав
Характеристики, полученные из матрицы совместной встречаемости	4	3. Отношение суммы главной диагонали D 0 матрицы совместной встречаемости между входным изображением и стегоизображением. 4. Отношение суммы диагонали D 1 матрицы совместной встречаемости между входным изображением и стегоизображением 5. Отношение суммы диагонали D 2 матрицы совместной встречаемости между входным изображением и стегоизображением 6. Отношение суммы диагонали D 3 матрицы совместной встречаемости между входным изображением и стегоизображением
Характеристики, связанные с HCF-COM разностной матрицы смежности (4 и 8 смежностей)	2	7. Соотношение COM-HCF значений разности соседних пикселей (DCOM-HCF) при 4-связной смежности между входным изображением и стегоизображением 8. Соотношение COM-HCF значений разности соседних пикселей (DCOM-HCF) при 8-связной смежности между входным изображением и стегоизображением
Характеристики, относящиеся к центральной части PDF	4	9. Соотношение наклона центральной части PDF при 4-х связной смежности между входным изображением и стегоизображением 10. Соотношение наклона центральной части PDF при 8-связной смежности между входным изображением и стегоизображением 11. Соотношение наклона центральной части PDF при 4-х связной смежности между входным изображением и стегоизображением, созданым по схеме 2LSB 12. Соотношение наклона центральной части PDF при 8-связной смежности между входным изображением и стегоизображением, созданым по схеме 2LSB

Классификатор

В качестве классификатора используется метод опорных векторов с ядром радиальной базисной функции (RBF). Коэффициент регуляризации скорректирован методом перекрёстной проверки.

Эффективность метода

Эффективность на предмет обнаружения вставок была протестирована на двух различных базах данных изображений. Результаты тестирования представлены в таблице 11.

Таблица 11. Эффективность обнаружения для двух наборов данных

Уровень встраивания, %	База данных изображений BOWS-2	База данных изображений UCID
100	96,26	90,96
75	92,50	86,39
50	85,51	78,36
25	74,53	63,62

Метод показывает высокую результативность. Ожидаемо, что эффективность обнаружения снижается по мере снижения уровня встраивания — до 96,26 % для максимального заполнения стегоконтейнера и до 74,53 % для 25 % уровня заполнения стегоконтейнера.

При этом предложенный метод показывает различия в результативности в зависимости от используемой базы данных – разница в эффективности обнаружения составляет от 6 почти до 11 % с возрастанием по мере снижения объёма заполняемости стегоконтейнера.

Также в работе произведено сравнение с другими методами стегоанализа. Результаты эксперимента приведены в таблице 12.

Таблица 12. Эффективность обнаружения для двух наборов данных

Уровень встраивания, %	Метод Хи-квадрата			Метод Хи-квадрата		
	WAM	DHCF-COMs # 1	DHCF-COMs # 2	WAM	DHCF-COMs # 1	DHCF-COMs # 2
100	91,50	94,51	88,73	81,72	85,48	76,31
75	88,27	92,75	77,25	4,63	83,28	66,42
50	83,24	84,47	63,78	61,57	74,63	63,44
25	72,21	70,23	56,61	43,44	56,56	56,52

Сравнивая показатели эффективности предложенного метода с другими методами, авторы делают вывод, что предложенная схема стегоанализа показывает лучшие результаты, особенно для набора изображений UCID.

2.5. Стегоанализ с использованием сигнатуры близкой цветовой пары

В работе [28] предложен метод стегоанализа для несжатого формата цветного изображения высокой плотности с использованием сигнатуры близкой цветовой пары.

Общая характеристика метода

В качестве сигнатуры используется соотношение близких цветовых пар и уникальных цветов. Метод основан на следующих подтверждённых гипотезах.

1. Для чистого несжатого изображения значение соотношения близких цветовых пар и уникальных цветов больше по сравнению с изображением, в которое встроено сообщение.
2. Если изображение не имеет встроенного сообщения, то после встраивания соотношение близких цветовых пар и уникальных цветов значительно уменьшается.
3. Если изображение уже является изображением со встроенным сообщением, то последующее встраивание не приведёт к значительному изменению этого соотношения. Данные утверждения протестированы с использованием 20 % стеговставки.

Эффективность метода

Эффективность измеряется через частоту ложных тревог (FAR) и частоту ложных обнаружений (FDR). Показано, что при выборе порога с фиксированным значением классификация будет вполне удовлетворительной по некоторым типам изображений (зелень, люди, объекты, водные объекты, земля и здания), но имеет высокую вероятность ошибочного обнаружения для классов других типов изображений (лица, небо и облака, животные).

Использование переменного порога, основанного на статистике изображений, повышает эффективность метода. Эффективность метода при использовании переменного порога представлена в таблице 13.

Таблица 13. Экспериментальные результаты, показывающие улучшение FAR и FDR в случае переменного порогового значения, %

Класс изображений	Частота ложных обнаружений (FDR)		Частота ложных тревог (FAR)	
	Постоянный порог	Переменный порог	Постоянный порог	Переменный порог
Лицо	88,88	0	5,56	5,56
Небо и облака	38,46	0	0	0
Животные	0	4,65	48,83	16,27

Так, согласно представленным результатам, применение переменного порога позволяет добиться отсутствия ложных обнаружений по таким классам, как «лицо» и «небо и облака» (что, по сути, даёт отсыл к такой цветовой гамме, как оттенки бежевого и синего), а также снижает частоту ложных тревог в классе «животные» в три раза, что также является существенным повышением точности предложенной модели. В тоже время следует отметить, что постоянный порог даёт несколько лучшие результаты по частоте ложных обнаружений

по сравнению с переменным порогом значений.

Отмечается, что алгоритм будет намного более надёжным, если порог автоматически выбран на основе статистики 1-го и 2-го порядка, включая плотность цвета и корреляцию пар пикселей.

2.6. Расширенная SRM-модель для стегоанализа цветных изображений

В работе [16] предлагается расширение SRM-модели для стегоанализа цветных изображений.

Общая характеристика метода

Модель имеет размерность 18157 и состоит из двух компонентов

1. Классическая SRM-модель с шагом квантования q = 1 (SRMQ1) с размерностью 12753 (4D-совпадения с порогом T = 2).
2. Дополнительные характеристики общей размерностью 4704 (совместные 3D-совпадения с порогом T = 3 и квантованием q = 1).

Встраиваемая полезная нагрузка – от 0,05 до 0,5 бит на пиксель канала.

Входные изображения подвергаются предварительной обработке, в результате чего авторы исследования получили три базы данных изображений для последующего обучения и тестирования:

1) изображения с изменением размера – BOSSbaseRes,
2) изображения с применением алгоритма демозаинга Patterned Pixel Grouping (PPG) — BOSSbasePPG,
3) изображения с применением алгоритма демозаинга Adaptive Homogenity-Directed (AHD) – BOSSbaseAHD.

Исследуемые характеристики (дополнительные)

В качестве характеристик, при помощи которых предлагается расширить классическую пространственнобогатую модель, используется набор трёхмерных сочетаний остатков, вычисленных по всем трём цветовым каналам.

Эти характеристики формируются из остаточных значений шума и вычисляются с использованием двух типов локальных предикторов пикселей:

1) линейных, вычисляемых путём свёртки изображения с помощью высокочастотного фильтра с инвариантным к сдвигу ядром (остатки «спама», размерность 700);
2) нелинейных, получаемых из остатков максимума / минимума выходов от нескольких линейных фильтров, разделённых на пять классов в зависимости от структуры фильтра: фильтры, использующие разности первого, второго и третьего порядка, граничные ядра и квадратичные ядра.

Классификатор

Используются бинарные классификаторы, реализованные с использованием ансамбля FLD с настройками по умолчанию, минимизирующего общую вероятность ошибки классификации.

Эффективность метода

Эффективность оценивается через среднюю ошибку обнаружения как функцию полезной нагрузки. Результаты проведенных экспериментов графически представлены на рисунках 1-3.

Общей закономерностью является снижение ошибок обнаружения по мере увеличения встраиваемой нагрузки. Также отмечается, что исходная модель SRMQ1 выдаёт наибольшую погрешность в базах данных с применением демозаинга, тогда как модель SCRMQ1, адаптированная для анализа цветных изображений с целью обнаружения встраиваемых сообщений, показывает существенно лучшие результаты для всех трёх баз изображений. Так, ошибки обнаружения моделей SRMQ1, CRMQ1 и SCRMQ1 составляют 0,0225, 0,0117 и 0,0080 соответственно.

Также отмечается, что подмодели с меньшими ядрами обычно обнаруживают лучше, чем большие ядра. Сделан вывод, что способ предварительной обработки изображения не оказывает большого влияния на эффективность модели.

2.7. Стегоанализ на основе сочетания пространственной и вейвлет-фильтрации

В работе [40] предлагается метод стегоатаки, основанный на совместном использовании пространственного и вейвлет-фильтров.

Общая характеристика метода

Метод использует дискриминантные функции на основе остатков, полученных с помощью пространственной (пространственный остаток) и вейвлет-фильтрации (вейвлет-остаток), а затем объединяет результаты двух дискриминантных функций для определения местоположения изменённых пикселей.

Модель позволяет определить местоположение модифицированных пикселей при 10 % уровне заполнения стегоконтейнера.

Алгоритм слияния остатков

Пространственный и вейвлет-остатки объединяются методом голосования.

На вход подаётся стегоизображение и вычисляется коэффициент модификации α , обозначающий соотношение изменённых пикселей и порог дискриминации.

Промежуточные действия включают высокочастотную фильтрацию изображения с использованием среднего значения по 4-м соседям для получения пространственного остатка, нахождение пространственных остаточных квадратов, вычисление одноуровневого вейвлет-разложения изображения с помощью 8-ступенчатого фильтра Добеши, обратное вейвлет-преобразование для получения окончательного остаточного изображения.

На выходе получается оценочная матрица модификации. Когда пиксель распознаётся как модифицированный пиксель, элементу присваивается значение 1; в противном случае ему присваивается значение 0.

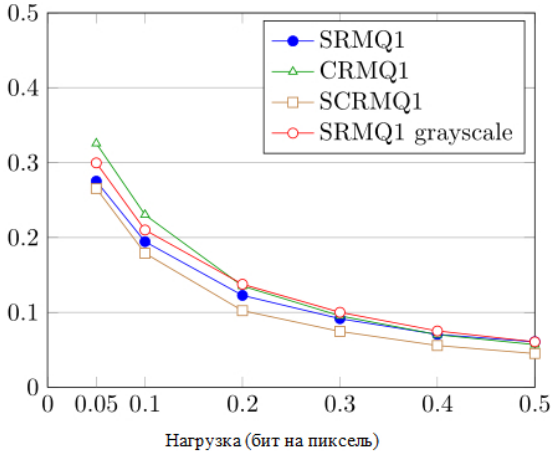

Рис. 1. Ошибка обнаружения как функция полезной нагрузки для трёх баз данных с использованием базы изображений BOSSbaseRes

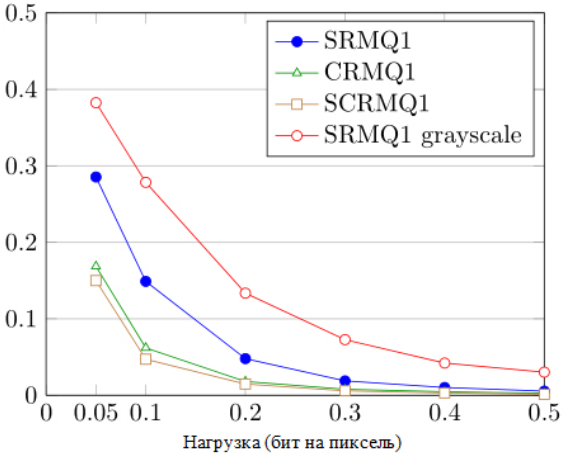

Рис. 2. Ошибка обнаружения как функция полезной нагрузки для трёх баз данных с использованием базы изображений BOSSbasePPG

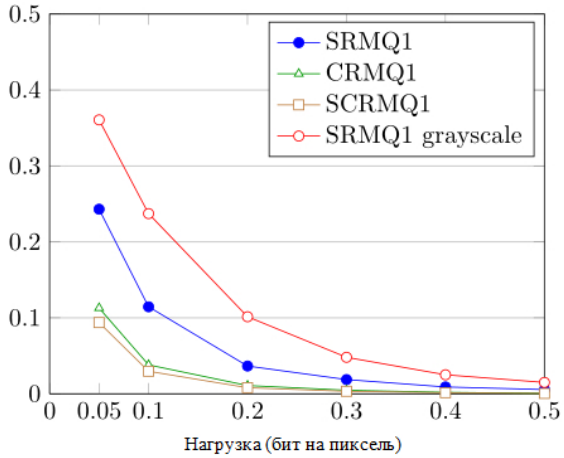

Рис. 3. Ошибка обнаружения как функция полезной нагрузки для трёх баз данных с использованием базы изображений BOSSbaseAHD

Эффективность метода

Эффективность алгоритма определяется через разницу между показателем истинно положительных и ложноположительных результатов. На основе тестирования 1000 изображений показывается значительно большая эффективность предложенного алгоритма по сравнению с использованием только пространственных или вейвлет-остатков.

2.8. Стегоанализ с применением топологических данных

В работе [30] описан метод стеганографческого анализа, основанного на концепции анализа топологических данных (TDA), связанных с определёнными характеристиками изображения.

Общая характеристика метода

Доказано, что разделение битов в соответствии с их образцами двоичного кода позволяет выявить присутствие определённых текстур путём построения симплициальных комплексов и сравнения количества связанных компонентов в последовательности возрастающих пороговых значений расстояния.

Метод разработан и апробирован для изображений в градациях серого. Входное изображение предварительно подвергается обработке с использованием mod16 для уменьшения диапазона значений пикселей от (0, ..., 255) до (0, ..., 15).

Исследуемая полезная нагрузка составляет 100 %.

Исследуемые характеристики

В качестве характеристик используются группы однородных локальных двоичных шаблонов (ULBP) (кодов ULBP) с дальнейшим построением возрастающей последовательности SC Rips, нулевые симплексы которой являются пикселями ориентиров ULBP из конечной возрастающей последовательности пороговых значений расстояний.

Отмечается, что для изображения в градациях серого существует 58 однородных LBP (ULBP) кодов. Исключив только нулевые или единичные шаблоны (00000000) и (11111111), оставшиеся 56 ULBP-кодов авторы разделяют на 7 групп, извлекая их в качестве симплексов, являющихся строительными блоками Rips SC.

Модель использует фиксированный набор пороговых значений расстояния $T\ i = 0, 4, 5, 7, 10, 15$, т. е. для каждого входного изображения будет вычислено 6 восьмимерных векторов признаков. Векторы извлекаются как для случая, когда коды ULBP содержат 6 единиц значений пикселей, так и для случая, когда коды ULBP содержат 3 единицы значений пикселей.

Эффективность метода

В таблицах 14 и 15 показаны средняя точность обнаружения стегоизображения для кодов ULBP с шестью и тремя единицами значений пикселей.

Таблица 14. Результаты классификации для кодов ULBP с шестью единицами значений пикселя, %

	T = 4	T = 5	T = 7	T = 10	T = 15
30 % Обучение	86,699	84,836	78,321	74,186	67,157
50 % Обучение	90,048	87,026	78,734	75,152	68,014
70 % Обучение	90,98	87,853	78,777	75,763	68,443
Обучение с исключением только одного изображения	92,7	88,7	79,1	75,8	68,132

Таблица 15. Результаты классификации для кодов ULBP с тремя единицами значений пикселя, %

	T = 4	T = 5	T = 7	T = 10	T = 15
30 % Обучение	86,449	84,46	87,234	78,306	66,573
50 % Обучение	89,382	84,882	88,738	79,578	68,338
70 % Обучение	90,43	85,213	89,54	80,133	69,24
Обучение с исключением только одного изображения	91,4	85,5	90,6	79,6	69,7

Представленные данные позволяют сделать вывод, что последовательность постоянных гомологических инвариантов может определять различия для целей стегоанализа с точностью более 90 %.

Метод позволяет обнаруживать стегоизображения с высокой точностью от первых пороговых значений, а затем постепенно уменьшать полученные результаты точности по мере его возрастания, что связано с увеличением размеров симплициальных комплексов.

Использование ULBP кода с 3-мя единицами значений пикселя приведёт к несколько более высокой точности классификации, по сравнению с ULBP кодом с 6-ю единицами значений пикселя.

3. Новейшие тенденции в стеганографическом анализе

Новейшей методологической основой стеганографического анализа стало использование технологии глубокого изучения. Так, в последние пять лет появилось большое количество работ, посвящённых возможностям использования сверточных нейронных сетей для обнаружения стеганографических вставок. Наиболее интересные работы в этой области приведены в таблице 16.

Таблица 16. Работы по изучению вопросов применения глубокого обучения и сверточных нейронных сетей в стегоанализе

Авторы	Год издания	Название работы
Xu G. et al [39]	2016	Ансамблевые CNN для целей стегоанализа: эмпирическое исследование
Xu G. et al [38]	2016	Структурный дизайн свёрточных нейронных сетей для стегоанализа
Ye J. et al [41]	2017	Иерархические представления глубокого обучения для стегоанализа изображений
Sharifzadeh M. et al [32]	2017	Применение свёрточного нейросетевого стегоанализа в стеганографии
Chen M. et al [6]	2018	Регрессоры глубокого обучения для количественного стегоанализа
Li B. et al [25]	2018	ReST-net: разнообразные модули активации и CNN на основе параллельных подсетей для стегоанализа пространственных изображений
Yedroudj M. et al [42]	2018	Yedroudj-net: эффективная CNN для пространственного стегоанализа
Zhang R. et al [45]	2018	Эффективное изучение функций и стегоанализ многоразмерных изображений на основе CNN

Продолжение таблицы 16

Авторы	Год издания	Название работы
Zhang T. et al [46]	2019	Новый метод стегоанализа изображений JPEG, сочетающий в себе особенности SRM-модели и свёрточных нейронных сетей
Cogranne R. et al [7]	2019	ALASKA-вызов в стегоанализе: первый шаг к стегоанализу
Kim J. et al [26]	2020	Стегоанализ изображений на основе CNN с использованием дополнительных данных
Wang Z. et al [34]	2020	Совместное многодоменное изучение функций для стегоанализа изображений на основе CNN
Eslam M. et al [10]	2020	Улучшение стегоанализа изображений на основе CNN на графических процессорах
Chaumont M. [5]	2020	Глубокое обучение в стеганографии и стегоанализе
You W. et al [43]	2020	Сиамские свёрточные нейронные сети для стегоанализа изображений
Soto R.T. et al [33]	2020	Стеганографический анализ цифровых медиа

Заключение

Следует отметить, что несмотря на многообразие имеющихся моделей стеганографического анализа, каждая имеет ряд ограничений, что вызывает необходимость разработки других, более совершенных (а значит, более эффективных) моделей.

Кроме того, появление новых методов и алгоритмов стеганографии является стимулом для дальнейшего развития. При этом наблюдается тенденция увеличения количества исследований, посвящённых вопросам стегоанализа, и существенный сдвиг методов стегоанализа на методы, связанные с применением свёрточных нейронных сетей. Предположительно, подобный сдвиг области исследований обусловлен развитием алгоритмов глубокого обучения и усовершенствования методов стеганографии и возрастанием их устойчивости к стегоатакам. В то же время предполагается сохранение актуальности любых других методов, направленных на обнаружение стеганографических вставок,

выполненных при помощи замены наименее значащих бит, что обусловлено простотой и, в связи с этим, широкой популярностью LSB-метода.

Литература

1. Al-Jarrah M., Al-Taei Z., Aboarqoub A. Steganalysis using LSB-focused statistical features // Proceedings of ICFNDS'17, Cambridge, United Kingdom, 2017, July 19-20, 5 pages. DOI: 10.1145/3102304.3109814.
2. Cancelli G., Doerr G., Cox I.J., Barni M. Detection of 1 LSB Steganography based on the Amplitude of Histogram Local Extrema // Int. Conf. Image Processing. 2008. P. 1288–1291.
3. Chaeikar A. Ensemble SW image steganalysis: A low dimension method for LSBR detection // Signal Process Image Commun. 2019. V. 70. P. 233–245.
4. Chaeikar. S.S., Ahmadi A. SW: A blind LSBR image steganalysis technique // Proceedings of the 10th International Conference on Computer Modeling and Simulation, Sydney Australia, 8 January 2018. P. 14–18.
5. Chaumont M. Deep learning in steganography and steganalysis // Digital Media Steganography, Academic Press. 2020. P. 321–349.
6. Chen M, Boroumand M, Fridrich J. Deep learning regressors for quantitative steganalysis // Electron Imaging 2018. V. 7. P. 160—161.
7. Cogranne R., Giboulot Q., Bas P. The ALASKA steganalysis challenge: A first step towards steganalysis // Proceedings of the ACM Workshop on Information Hiding and Multimedia Security, 2019. P. 125–137.
8. Dumitrescu S., et al. Detection of lsb steganography via sample pair analysis // IEEE Trans. Signal Process. 2003. V. 51, No. 7. P. 1995-–2007.
9. Dumitrescu S., Wu X. A new framework of lsb steganalysis of digital media // IEEE Trans. Signal Process. 2005. V. 53. P. 3936-–3947.
10. Eslam M., Elshafey M.A., Mohamed M. Fouad. Enhancing CNN-based Image Steganalysis on GPUs // Journal of Information Hiding and Multimedia Signal Processing. 2020. V. 11, No. 3. P. 138–150.
11. Fridrich J, Kodovsky J. Rich models for steganalysis of digital images // IEEE Transactions on Information Forensics and Security. 2012. V. 7. P. 868–882.
12. Fridrich J., et al., Steganalysis of LSB encoding in colour image // Proc. 2000 IEEE International Conference on Multimedia and Expo, New York, USA. 2000 V. 3, P. 1279–1282.
13. Fridrich J., Goljan M., Du R. Reliable detection of LSB steganography in color and grayscale images // Proceedings of the 2001 workshop on Multimedia and security: new challenges, ACM. 2001. P. 27–30.
14. Fridrich J., Goljan M., Soukal D. Higher-order statistical steganalysis of palette images // Proc. SPIE, EI. 2003. V. 5020. P. 178–190.
15. Goljan M., Fridrich J., Holotyak T. New Blind Steganalysis and its Implications // SPIE Security, Steganography and watermarking of Multimedia Contents. 2006. V. 6072. P. 1–13.
16. Goljan, M., Fridrich, J., Cogranne, R. Rich model for steganalysis of color images // Information Forensics and Security (WIFS), 2014 IEEE International Workshop. 2014. P. 185–190.

17. Gul G., Kurugollu F., SVD-based universal spatial domain image steganalysis // IEEE Transactions on Information Forensics and Security. 2010. V. 5. P. 349–353.
18. Harmsen J., Pearlman W. Steganalysis of additive noise modelable information hiding // Proc. of SPIE. 2003. V. 5020. P. 131–142.
19. Juarez-Sandoval O., Cedillo-Hernandez M., Sanchez-Perez G. et all. Compact Image Steganalysis for LSB-Matching Steganography // 5th International Workshop on Biometrics and Forensics (IWBF). 2017. P. 1–6.
20. Ker A.D. Improved Detection of LSB Steganography in Grayscale Images // International Workshop on Information Hiding, IH. 2004. P. 97–115.
21. Ker A.D. Resampling and the detection of LSB matching in color bitmaps // Proc. SPIE, EI. 2005. V. 5681. P. 1–15.
22. Ker A.D. Steganalysis of LSB matching in grayscale images // IEEE signal processing letters. 2005. V. 12. P. 441–444.
23. Kim J, Park H, Park J.-I. CNN-based image steganalysis using additional data embedding // Multimed Tools Appl. 2020. V. 79. P. 1355—1372.
24. Kumar U.P., Shankar D.D. Blind Steganalysis for JPEG Image susing SVM and SVM-PSO Classifiers // International Journal of Innovative Technology and Exploring Engineering (IJITEE). 2019. V. 8. P. 1239–1246.
25. Li B., Wei W., Ferreira A, Tan S. ReST-net: diverse activation modules and parallel subnets-based CNN for spatial image steganalysis // IEEE Signal Process Lett. 2018. V. 25, No. 5. P. 650—654.
26. Lyu S., Farid H. Detecting hidden messages using higher order statistics and support vector machines // Proceedins of Lecture Notes in Computer Science: 5th International Workshop on Information Hiding. 2002. V. 2578. P. 340–354.
27. Lyu S., Farid H. Steganalysis using color wavelet statistics and one-class support vector machines // In Proc. SPIE, EI, 2004. V. 5306. P. 35—45.
28. Mitra S., Roy T., Mazumdar D., Saha A.B. Steganalysis of LSB encoding in uncompressed images by close colour pair analysis // IIT Kanpur Hackers' Workshop 2004(IITK-HACK04). 23–24 Feb. 2004.
29. Pevny T., Patrick B., Fridrich J. Steganalysis by subtractive pixel adjacency matrix // IEEE Transactions on information Forensics and Security. 2010, February. V. 5, P. 215–224.
30. Rashid R.D., Asaad A., Jassim S. Topological Data Analysis as Image Steganalysis Technique // Mobile Multimedia/Image Processing, Security, and Applications. 2018. V. 10668. P. 17–26.
31. Shankar D.D., Azhakath A.S. Minor blind feature based Steganalysis for calibrated JPEG images with cross validation and classification using SVM and SVM-PSO // Multimedia Tools and Applications. 2020. DOI: 10.1007/s11042-020-09820-7.
32. Sharifzadeh M., Agarwal C., Aloraini M., Schonfeld D. Convolutional neural network steganalysis's application to steganography // IEEE Visual Communications and Image Processing. Dec 2017. P. 1–4.
33. Soto R.T., Ramos-Pollan R., Isazad G., et al. Digital media steganalysis. Digital Media Steganography: Principles, Algorithms, and Advances // ElsevierISBN: 9780128194386. DOI: 10.1016/C2018-0-04865-3. 2020. P. 259-293.
34. Wang Z., Chen M., Yang Y. Joint multi-domain feature learning for image steganalysis based on CNN // EURASIP Journal on Image and Video Processing. 2020(1). DOI:

10.1186/s13640-020-00513-7.
35. Westfeld A. Detecting low embedding rates // Proc. IHW. 2002. V. 2578 of LNCS. P. 324—339.
36. Westfeld A., Pfitzmann A. Attacks on Steganographic Systems // Proceedings of Lecture Notes in Computer Science. 2000. V. 1768. P. 61–75.
37. Westfeld A., Pfitzmann A. Attacks on steganographic systems // International workshop on information hiding, Springer. 1999. P. 61–76.
38. Xu G., Wu H.Z., Shi Y.Q. Structural design of convolutional neural networks for steganalysis // IEEE Signal Process. Lett. 2016. V. 23, No. 5. P. 708–712.
39. Xu G., Wu H-Z., Shi YQ. Ensemble of CNNs for steganalysis: An empirical study // Proceedings of the 4th ACM Workshop on Information Hiding and Multimedia Security. 2016. P. 103—107.
40. Yang C., Wang J. Lin C. Chen H., Wang W. Locating Steganalysis of LSB Matching Based on Spatial and Wavelet Filter Fusion // CMC-Comput. Mat. Contin. 2019. V. 60, No. 2. P. 633-–644.
41. Ye J., Ni J., Yi Y. Deep learning hierarchical representations for image steganalysis // IEEE Trans Inf Forensics Secur. 2017. V. 12, No. 11. P. 2545-–255.
42. Yedroudj M., Comby F., Chaumont M. Yedroudj-net: An efficient CNN for spatial steganalysis // IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP). 2018. P. 2092–2096.
43. You W, Zhang H., ZhaoX. A Siamese CNN for Image Steganalysis // IEEE Transactions on Information Forensics and Security. 2020. V. 16. P. 291–306.
44. Zhang J., et al., Steganalysis for LSB matching in images with high-frequency noise // Proc. MMSP 2007, Crete, Greece. 2007. P. 385-–388.
45. Zhang R., Zhu F., Liu J., Liu G. Efficient feature learning and multi-size image steganalysis based on CNN // arXiv Prepr. arXiv1807.11428. 2018.
46. Zhang T, Zhang H, Wang R, Wu Y. A new JPEG image steganalysis technique combining rich model features and convolutional neural networks // Math Biosci Eng. 2019. V. 16, No. 5. P. 4069-–4081.

A SURVEY OF STEGANALYSIS METHODS IN THE PAPERS OF FOREIGN AUTHORS

D.E. Vilkhovskiy
Assistant of the Department of Information Security, e-mail: vilkhovskiy@gmail.com

Dostoevsky Omsk State University, Omsk, Russia

Abstract. The paper provides a survey of foreign studies regarding steganalysis, aimed to detect hidden message insertion made by applying least significant bit replacement and discrete cosine transform algorithms. It is noted the further steganalysis methodology development splits in two directions: a decrease of the complexity and cost of processing and detection while maintaining a high level of classification rate, which is quite justified in the case of the presence of insertions with a large payload, i.e. up to 100%; or an increase of the insert recognition efficiency when dealing with images of a low payload. Besides, during the last five years, steganalisys

methods based on machine learning and deep learning began to play a dominant role in steganalysis

Keywords: steganalysis, steganographic analysis, LSB insertion, least significant bit replacement method.

References

1. Al-Jarrah M., Al-Taei Z. and Aboarqoub A. Steganalysis using LSB-focused statistical features. Proceedings of ICFNDS'17, Cambridge, United Kingdom, 2017, July 19-20, 5 pages. DOI: 10.1145/3102304.3109814.
2. Cancelli G., Doerr G., Cox I.J., and Barni M. Detection of 1 LSB Steganography based on the Amplitude of Histogram Local Extrema. Int. Conf. Image Processing, 2008, pp. 1288–1291.
3. Chaeikar A. Ensemble SW image steganalysis: A low dimension method for LSBR detection. Signal Process Image Commun., 2019, vol. 70, pp. 233–245.
4. Chaeikar. S.S. and Ahmadi A. SW: A blind LSBR image steganalysis technique. Proceedings of the 10th International Conference on Computer Modeling and Simulation, Sydney Australia, 8 January 2018, pp. 14–18.
5. Chaumont M. Deep learning in steganography and steganalysis. Digital Media Steganography, Academic Press, 2020, pp. 321–349.
6. Chen M, Boroumand M, and Fridrich J. Deep learning regressors for quantitative steganalysis. Electron Imaging, 2018, vol. 7, pp. 160—161.
7. Cogranne R., Giboulot Q., and Bas P. The ALASKA steganalysis challenge: A first step towards steganalysis. Proceedings of the ACM Workshop on Information Hiding and Multimedia Security, 2019, pp. 125–137.
8. Dumitrescu S., et al. Detection of lsb steganography via sample pair analysis. IEEE Trans. Signal Process, 2003, vol. 51, no. 7, pp. 1995-–2007.
9. Dumitrescu S. and Wu X. A new framework of lsb steganalysis of digital media. IEEE Trans. Signal Process, 2005, vol. 53, pp. 3936-–3947.
10. Eslam M., Elshafey M.A., and Mohamed M. Fouad. Enhancing CNN-based Image Steganalysis on GPUs. Journal of Information Hiding and Multimedia Signal Processing, 2020, vol. 11, no. 3, pp. 138–150.
11. Fridrich J and Kodovsky J. Rich models for steganalysis of digital images. IEEE Transactions on Information Forensics and Security, 2012, vol. 7, pp. 868–882.
12. Fridrich J., et al., Steganalysis of LSB encoding in colour image. Proc. 2000 IEEE International Conference on Multimedia and Expo, New York, USA, 2000, vol. 3, pp. 1279–1282.
13. Fridrich J., Goljan M., and Du R. Reliable detection of LSB steganography in color and grayscale images. Proceedings of the 2001 workshop on Multimedia and security: new challenges, ACM, 2001, pp. 27–30.
14. Fridrich J., Goljan M., and Soukal D. Higher-order statistical steganalysis of palette images. Proc. SPIE, EI., 2003, vol. 5020, pp. 178–190.
15. Goljan M., Fridrich J., and Holotyak T. New Blind Steganalysis and its Implications, SPIE Security, Steganography and watermarking of Multimedia Contents, 2006, vol. 6072, pp. 1–13.

16. Goljan, M., Fridrich, J., and Cogranne, R. Rich model for steganalysis of color images. Information Forensics and Security (WIFS), 2014 IEEE International Workshop, 2014, pp. 185–190.
17. Gul G. and Kurugollu F., SVD-based universal spatial domain image steganalysis. IEEE Transactions on Information Forensics and Security, 2010, vol. 5, pp. 349–353.
18. Harmsen J. and Pearlman W. Steganalysis of additive noise modelable information hiding. Proc. of SPIE, 2003, vol. 5020, pp. 131–142.
19. Juarez-Sandoval O., Cedillo-Hernandez M., Sanchez-Perez G. et all. Compact Image Steganalysis for LSB-Matching Steganography. 5th International Workshop on Biometrics and Forensics (IWBF), 2017, pp. 1–6.
20. Ker A.D. Improved Detection of LSB Steganography in Grayscale Images. International Workshop on Information Hiding, IH, 2004, pp. 97–115.
21. Ker A.D. Resampling and the detection of LSB matching in color bitmaps. Proc. SPIE, EI, 2005, vol. 5681, pp. 1–15.
22. Ker A.D. Steganalysis of LSB matching in grayscale images. IEEE signal processing letters, 2005, vol. 12, pp. 441–444.
23. Kim J, Park H, and Park J.I. CNN-based image steganalysis using additional data embedding. Multimed Tools Appl., 2020, vol. 79, pp. 1355—1372.
24. Kumar U.P. and Shankar D.D. Blind Steganalysis for JPEG Image susing SVM and SVM-PSO Classifiers. International Journal of Innovative Technology and Exploring Engineering (IJITEE), 2019, vol. 8, pp. 1239–1246.
25. Li B., Wei W., Ferreira A, and Tan S. ReST-net: diverse activation modules and parallel subnets-based CNN for spatial image steganalysis. IEEE Signal Process Lett., 2018, vol. 25, no. 5, pp. 650—654.
26. Lyu S. and Farid H. Detecting hidden messages using higher order statistics and support vector machines. Proceedins of Lecture Notes in Computer Science: 5th International Workshop on Information Hiding, 2002, vol. 2578, pp. 340–354.
27. Lyu S. and Farid H. Steganalysis using color wavelet statistics and one-class support vector machines. In Proc. SPIE, EI, 2004, vol. 5306, pp. 35—45.
28. Mitra S., Roy T., Mazumdar D., and Saha A.B. Steganalysis of LSB encoding in uncompressed images by close colour pair analysis. IIT Kanpur Hackers' Workshop 2004(IITK-HApp. 04), 23–24 Feb. 2004.
29. Pevny T., Patrick B., and Fridrich J. Steganalysis by subtractive pixel adjacency matrix. IEEE Transactions on information Forensics and Security, 2010, February, vol. 5, pp. 215–224.
30. Rashid R.D., Asaad A., and Jassim S. Topological Data Analysis as Image Steganalysis Technique. Mobile Multimedia/Image Processing, Security, and Applications, 2018, vol. 10668, pp. 17–26.
31. Shankar D.D. and Azhakath A.S. Minor blind feature based Steganalysis for calibrated JPEG images with cross validation and classification using SVM and SVM-PSO. Multimedia Tools and Applications, 2020. DOI: 10.1007/s11042-020-09820-7.
32. Sharifzadeh M., Agarwal C., Aloraini M., and Schonfeld D. Convolutional neural network steganalysis's application to steganography. IEEE Visual Communications and Image Processing, Dec 2017, pp. 1–4.
33. Soto R.T., Ramos-Pollan R., Isazad G., et al. Digital media steganalysis. Digital Media Steganography: Principles, Algorithms, and Advances, ElsevierISBN: 9780128194386.

DOI: 10.1016/pp. 018-0-04865-3. 2020. P. 259-293.
34. Wang Z., Chen M., and Yang Y. Joint multi-domain feature learning for image steganalysis based on CNN. EURASIP Journal on Image and Video Processing, 2020 (1). DOI: 10.1186/s13640-020-00513-7.
35. Westfeld A. Detecting low embedding rates. Proc. IHW, 2002, vol. 2578 of LNCS, pp. 324—339.
36. Westfeld A. and Pfitzmann A. Attacks on Steganographic Systems. Proceedings of Lecture Notes in Computer Science, 2000, vol. 1768, pp. 61–75.
37. Westfeld A. and Pfitzmann A. Attacks on steganographic systems. International workshop on information hiding, Springer, 1999, pp. 61–76.
38. Xu G., Wu H.Z., Shi Y.Q. Structural design of convolutional neural networks for steganalysis, IEEE Signal Process. Lett. 2016. V. 23, No. 5. P. 708–712.
39. Xu G., Wu H-Z. and Shi YQ. Ensemble of CNNs for steganalysis: An empirical study. Proceedings of the 4th ACM Workshop on Information Hiding and Multimedia Security, 2016, pp. 103—107.
40. Yang C., Wang J. Lin C. Chen H., and Wang W. Locating Steganalysis of LSB Matching Based on Spatial and Wavelet Filter Fusion. CMC-Comput. Mat. Contin., 2019, vol. 60, no. 2, pp. 633-–644.
41. Ye J., Ni J., and Yi Y. Deep learning hierarchical representations for image steganalysis. IEEE Trans Inf Forensics Secur., 2017, vol. 12, no. 11, pp. 2545-–255.
42. Yedroudj M., Comby F., and Chaumont M. Yedroudj-net: An efficient CNN for spatial steganalysis. IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), 2018, pp. 2092-–2096.
43. You W, Zhang H., and ZhaoX. A Siamese CNN for Image Steganalysis. IEEE Transactions on Information Forensics and Security, 2020, vol. 16, pp. 291–306.
44. Zhang J., et al., Steganalysis for LSB matching in images with high-frequency noise. Proc. MMSP 2007, Crete, Greece, 2007, pp. 385-–388.
45. Zhang R., Zhu F., Liu J., and Liu G. Efficient feature learning and multi-size image steganalysis based on CNN. arXiv Prepr. arXiv1807.11428, 2018.
46. Zhang T, Zhang H, Wang R, and Wu Y. A new JPEG image steganalysis technique combining rich model features and convolutional neural networks. Math Biosci Eng., 2019, vol. 16, no. 5, pp. 4069-–4081.

Дата поступления в редакцию: 23.11.2020