УДК 621.391

СИГНАТУРА БЛИЗКОЙ ЦВЕТОВОЙ ПАРЫ В СТЕГОАНАЛИЗЕ

Ковынёв Н.В.

Московский государственный технический университет им. Н.Э. Баумана
Москва, Российская Федерация

Аннотация. В данной статье рассматривается способ применения комбинированного метода обнаружения стегосообщений в изображениях.
Ключевые слова: стегоанализ, стеганография, изображение, сокрытие.

THE SIGNATURE OF A CLOSE COLOR PAIR IN STEGANALYSIS

Kovynyov N.

Bauman Moscow State Technical University
Moscow, Russia

Abstract. This article discusses about approach of applying method of detecting stego in images.
Keywords: steganalysis, steganography, image, concealment.

Адрес для переписки: Ковынёв Н.В. 2я Бауманская улица, д.5 стр.1, 105005, Москва, Российская Федерация
e-mail: nvkovynyov@bmstu.ru, n.kovynyov@gmail.com

Задача стеганографии – сокрытие факта передачи информации, которая встроена в любой мультимедийный контейнер (файл): изображение, аудиофайл, видеофайл. Особенностью скрытой передачи информации является факт сокрытия встраивания информации в мультимедийный файл. Стегоанализ же, напротив, имеет задачу обнаружения факта встраивания стегосообщений в мультимедийные контейнеры. Являясь противоположностями друг друга, данные направления находятся в непрерывном развитии, каждый в своем случае.

Во многих случаях стегоанализа используются универсальные методы, которые иногда называют слепыми. Особенность данных меодов является эффективная работа при любых слепых схемах встраивания, иными словами: алгоритмы и схемы встраивания известны только автору стегосообщения.

В данной работе описан метод стегоанализа с использованием сигнатуры близкой цветовой пары. Данный метод стегоанализа работает на обнаружение встраиваний в мультимедийные файлы способом замены наименее значащих битов (Least Significant Bit,LSB). Данный метод наиболее распространен в электронной стеганографии. Он основан на ограниченных возможностях человеческих органов чувств, в силу которых люди не способны различать незначительные вариации цветов или звуков. Модификации метода LSB довольно популярны в стеганографии, особенно популярен данный способ с изображениями формата JPEG. Где сжатие происходит практически без потерь, потому что скорытие происходит в младших разрядах коэффициентов, связанных с пользовательской информацией. В результате этого данные методы обладают некоторыми преимуществами, а именно: мультимедиа контейнеры не вызывают подозрений, можно спокойно пересылать изображения; младшие биты оцифрованных изображений могут иметь различное распределение в зависимости от применявшихся параметров аналого-цифрового преобразования, от дополнительной обработки и от прочих факторов, что делает данный метод наиболее защищенным от обнаружения вложений; реализация не требует множества временных и мощностных ресурсов, так как сама идея довольно проста и эффективна.

Контейнером в случае сигнатуры близкой цветовой пары является цветное изображение высокой плотности, которое не сжато.

В данном методе в качестве сигнатуры используется соотношение близких цветовых пар и уникальных цветов. Метод базируется на подтвержденных гипотезах:

Соотношение близких цветовых пар и уникальных цветов исходного (без стегосообщения) несжатого изображения больше, чем у изображения, которое содержит в себе стегосообщение (встроенное сообщение).

После встраивания стегосообщения в изображение, уменьшается соотношение близких цветовых пар и уникальных цветов в данном изображении.

Если в изображении уже содержится стегосообщение (скрытое встроенное сообщение), то последующие встраивания значительно не изменят соотношение близких цветовых пар и уникальных цветов. Однако, данное утверждение на практике протестировано для малого процента стеговставок.

Эффективность метода измеряется при помощи частоты ложных тревог (False Alarm Rate, FAR) и частоты ложных обнаружений (False Discovery Rate, FDR). Если выбрать порог с фиксированным значением, классификация будет удовлетворительной по некоторым типам устойчивых изображений (земля, здания, объекты, люди), но присутствует высокая вероятность ошибочного обнаружения для клас-

сов других типов изображений (лица, небо и облака, животные).

При использовании переменного порога значений, который основан на статистике изображений, повышается эффективность данного метода, что можно увидеть в табл. 1 и 2.

Таблица 1. FDR при использовании переменного порога значений

Класс изображений	Частота ложных обнаружений (FDR)	
	Переменный порог	Переменный порог
Лицо	87	0
Небо и облака	37	0
Животные	0	4,5

Таблица 2. FAR при использовании переменного порога значений

Класс изображений	Частота ложных тревог (FAR)	
	Постоянный порог	Переменный порог
Лицо	5,5	5,5
Небо и облака	0	0
Животные	47	16

По результатам, представленным в таблицах 1 и 2, видно, что применение переменного порога позволяет исключить ложные обнаружения по следующим классам, а именно: лицо, небо и облака (или цветовые оттенки бежевого и синего). Также, следует отметить, что применение переменного порога снижает частоту ложных тревог в классе животные, что существенно повышает точность данного метода. Однако, следует заметить, что постоянный порог дает более высокие результаты по частоте ложных обнаружений при сравнении с переменным порогом значений.

В заключении стоит отметить, что повышение надежности данного способа стегоанализа можно достичь путем использования выбора порога на основе статистики первого и второго порядка, куда также будет включена плотность цвета и корреляция пикселей, что позволит наиболее эффективно проводить анализ наименее значащих битов в графических изображениях. Стоит отметить, что актуальность по разработке методов стегоанализа относительно методов наименее значащих битов сохранится в виду того, что данный метод стеганографии довольно прост и не требует много ресурсов при его реализации, что обуславливает его популярность. Несмотря на популярность алгоритмов стеганографии, основанных на методе LSB, не стоит забывать об алгоритмах, которые построены на основе глубокого обучения, которые реализуются применением сверточных нейронных сетей.

Литература

1. Вильховский, Д. Э. Обзор методов стеганографического анализа изображений в работах зарубежных авторов / Д. Э. Вильховский // Математические структуры и моделирование. – 2020. – С. 75–102.

2. Steganalysis of LSB encoding in uncompressed images by close colour pair analysis / S. Mitra [et al.] // IIT Kanpur Hackers' Workshop 2004 (IITK-HACK04), 2004.

3. Бирюков А Стеганография: реализация и предотвращение / А. Бирюков // Системный администратор. – 2015. – С. 24–27.

4. Кочергина, М. А. Стеганография. Метод замены наименее значащего бита / М. А. Кочергина, Н. В. Первов ; под редакцией Калмыкова Б. М. – Чебоксары : Чувашский государственный университет имени И.Н. Ульянова, – 2014. – С. 86–89.

УДК 535.39

КОМПОЗИТНЫЕ МАТЕРИАЛЫ ДЛЯ СИСТЕМ ЗАЩИТЫ ОТ ЭЛЕКТРОМАГНИТНЫХ ИЗЛУЧЕНИЙ

Кольчевская М.Н., Парфимович И.Д., Комаров Ф.Ф.

НИУ «Институт прикладных физических проблем имени А. Н. Севченко» БГУ
Минск, Республика Беларусь

Аннотация. Разработка широкополосных экранирующих композитных материалов на основе полимеров, наполненных углеродными наноструктурами, для защиты от электромагнитных излучений, обладающих: высокой износостойкостью, твердостью, селективностью коэффициентов отражения и поглощения электромагнитных излучений в широком спектральном диапазоне, а также снижающих массогабаритное соотношение.

Ключевые слова: углеродные нанотрубки, композитные материалы, антибликовые материалы, радиопоглощающие материалы, безэховые камеры.