5. Неправильная сортировка слоев.

Возможна ситуация, когда элементы нижних слоев элемента помещаются выше и перекрывают другие важные части. Такое возможно если используются несколько страниц атласа. Этому можно противодействовать, добавив компонент Sorting Group в каркас GameObject. Другим обходным решением является поворот камеры на небольшую величину, например, установите значение Y поворота преобразования камеры равным 0,001.

6. Скелет выглядит в Unity розовым.

Вероятнее всего в материале используется неверный шейдер. Пакет рекомендуемых шейдеров доступен к скачиванию на сайте разработчика Spine.

Для увеличения производительности будет полезным выполнение следующих рекомендаций.

1. По возможности избегайте использования обрезки полигонов, рассмотрите вместо этого использование функций маскирования Unity.

2. Используйте как можно меньше ключей деформации сетки.

3. Используйте как можно меньше вершин.

4. Удалите ненужные ключи.

5. Используйте как можно меньше текстур страниц атласа.

6. Если для скелета требуется несколько материалов, попробуйте оптимизировать порядок прорисовки в Spine, чтобы свести к минимуму количество переключателей материалов.

В случае если возникшие трудности не удалось решить, то разработчик дает возможность оставить свой вопрос на форуме.

ЛИТЕРАТУРА

1. Esotericsoftware [Электронный ресурс]. – Режим доступа: http:// ru.esotericsoftware.com / – Дата доступа: 19.02.2023.

УДК 004.56+003.26

Асп. Н.В. Попеня, доц. Д.М. Романенко
(БГТУ, г. Минск)

ОСОБЕННОСТИ ПРИМЕНЕНИЯ СТЕГАНОГРАФИЧЕСКИХ МЕТОДОВ ДЛЯ ВИДЕОФАЙЛОВ

В настоящее время в связи с постоянно ускоряющимся развитием цифровых глобальных высокоскоростных сетей передачи данных большой интерес приобретает задача защиты мультимедийного контента от незаконного распространения.

Современная цифровая стеганография помимо своего основного

направления – скрытой передачи данных, может быть использована для защиты авторских прав, контента. В таком случае ее цель меняется – скрытое сообщение становится «водяным знаком», зачастую невидимым, с помощью которого возможно идентифицировать автора или владельца информации [1]. Стеганография является достаточно мощным инструментом сохранения конфиденциальности информации, а ее применение давно признано эффективным средством защиты не только авторских прав, но и любой информации, которая относится к интеллектуальной собственности.

Применение стеганографических методов для видеофайлов привлекает все больше внимания не только из-за роста требований к обеспечению безопасности, но и из-за того, что использование видеофайлов становится более предпочтительным. Можно выделить основную причину этого явления – средний размер видеофайла больше среднего размера иных мультимедиа-объектов (изображения, аудио, текстуры 3D-объектов), что дает возможность внедрить большее количество информации в стегоконтейнер.

Видеофайл обычно состоит из контейнера, содержащего видеоданные в формате кодирования видео вместе с аудиоданными в формате аудиокодирования. Контейнер также может содержать информацию о синхронизации, субтитры и метаданные, такие как заголовок.

Видеоданные представляют собой серию цифровых изображений, отображаемых в быстрой последовательности. В контексте видео эти изображения называются кадрами. Скорость отображения кадров известна как частота кадров и измеряется в кадрах в секунду (FPS). Каждый кадр является ортогональным растровым цифровым изображением и, следовательно, содержит растр пикселей.

Как правило, для сокрытия информации в видеофайлах используются методы, использующие только видеоданные. Наименее распространенными методами являются те, которые используют аудиоданные в видеофайлах. В настоящее время используются следующие алгоритмы внедрения информации в аудиоинформацию:

– метод расширения спектра, в котором происходит незначительное изменение амплитуды каждого отсчета аудиосигнала;

– модификация фазы аудиосигнала, при котором начальный сегмент аудио модифицируется в зависимости от внедряемых данных;

– изменение времени задержки эхо-сигнала.

На стойкость стеганографической системы критическое влияние оказывает правило выбора элементов стеганографического контейнера, модифицируемых в процессе встраивания информации [2]. При использовании видеоданных в качестве стегоконтейнера следует отметить следующую особенность: если размер скрываемой информа-

ции небольшой по сравнению с объемом контейнера, то можно вносить изменения не в каждый кадр, а с некоторым интервалом. Это может затруднить обнаружение факта сокрытия информации с помощью методов статистического стегоанализа.

Встраивание информации в видеоданные может осуществляться как в информационную часть, так и в область служебных полей файла (так называемые форматные методы). Каждый метод обладает своими особенностями: вложение непосредственно в информационную часть позволяет передать значительный объем данных, пропорциональный исходному размеру контейнера, но обнаруживается методами статистического анализа, а также является хрупким для операций масштабирования, редактирования и конвертации. Форматные методы потенциально стойки к методам статанализа и проведению указанных операций с файлами (при определенных условиях), но позволяют скрытно передать весьма небольшие объемы информации, а также обладают крайне низкой стойкостью к операциям анализа структуры файла [3].

Можно выделить следующие способы внедрения сообщения в информационную часть видеофайла: встраивание на уровне коэффициентов, на уровне битовой плоскости и за счет энергетической разницы между коэффициентами.

При использовании метода встраивания информации на уровне коэффициентов биты скрываемой информации встраиваются в коэффициенты дискретного косинусного преобразования (ДКП). Главной проблемой модификации коэффициентов ДКП в сжатом потоке видео является накопление сдвига или ошибок. Искажения, вызванные изменением коэффициентов ДКП, могут распространяться во временной и в пространственной областях. При использовании данного метода скрываемая информация сохраняется при фильтровании, зашумлении (аддитивным шумом) и дискретизации.

Метод встраивания информации на уровне битовой плоскости отличается высокой пропускной способностью и небольшой вычислительной сложностью. Но есть и существенный недостаток: информация, встроенная таким образом, может быть легко удалена. При повторном наложении последовательности бит качество видео ухудшится незначительно, а скрываемая информация будет уничтожена.

В основе метода встраивания информации за счет энергетической разницы между коэффициентами лежит дифференциальное встраивание энергии (ДЭВ). Сложность алгоритма ДЭВ незначительно выше сложности метода встраивания на уровне битовой плоскости. Метод ДЭВ может быть применен не только к видеоданным MPEG, но и к другим алгоритмам сжатия видео. Информация встраивается

путем удаления нескольких коэффициентов ДКП. Алгоритм ДЭВ вносит в видео несколько меньше искажений, чем метод встраивания информации на уровне битовой плоскости. Для удаления скрытой информации требуется проведение более сложных вычислительных операций, чем встраивание новой произвольной битовой последовательности [4].

Стегоконтейнер может подвергается атакам, которые будут направлены на удаление или подмену скрываемой информации в видеоданных. Используются следующие виды атак:

– перекодирование видео с использованием алгоритмов сжатия с потерями (компрессия и видео с помощью кодеков изображения);

– изменение порядка кадров исходной видеопоследовательности (удаление одного или нескольких кадров, изменение частоты кадров, вырезание определенного временного отрезка видео);

– геометрические преобразования (изменение размеров кадра, изменение разрешения изображения, сжатие-растяжение).

ЛИТЕРАТУРА

1. Евсютин О.О., Кокурина А.С. Обзор методов встраивания информации в цифровые объекты для обеспечения безопасности в «интернете вещей» // Компьютерная оптика. – 2019. – № 1 (43). – С. 137-154.

2. Разинков Е.В., Латыпов Р.Х. О правиле выбора элементов стеганографического контейнера в скрывающем преобразовании // Прикладная дискретная математика. – 2010. – № 3. – С. 39-41.

3. Радаев С.В., Басов О.О., Мясин К.И., Мотиенко А.И. Встраивание стеганографических сообщений в видеофайлы формата MPEG-4 // Экономика. Информатика. – 2018. – № 4. – С. 773-785.

4. Моденова О.В. Стеганография и стегоанализ в видеофайлах // Прикладная дискретная математика. – 2010. – № 3. – С. 37-39.

УДК 004.56+003.26

Асп. Н.В. Попеня
(БГТУ, г. Минск)

МЕТОДЫ ЗАЩИТЫ АВТОРСКИХ ПРАВ НА ВИДЕОИНФОРМАЦИЮ

В настоящее время наблюдается проблема неограниченного неавторизованного копирования видеофайлов. Важной проблемой является определение подлинности полученной информации, то есть ее аутентификация.

Основное требование, которому должна отвечать система защи-