УДК 004.56+003.26

Н.В. Попеня, асп.; Д.М. Романенко, доц., канд. техн. наук
(БГТУ, г. Минск)

МОДИФИКАЦИЯ АЛГОРИТМОВ СТЕГАНОГРАФИЧЕСКИХ ПРЕОБРАЗОВАНИЙ ДЛЯ ВИДЕОФАЙЛОВ С УЧЕТОМ ОСОБЕННОСТЕЙ КОДЕКОВ

Стеганография – это метод скрытия информации в другом объекте, называемом носителем. Видеофайлы являются одним из популярных контейнеров для стеганографии, поскольку они обладают большой емкостью и могут содержать скрытые данные без заметного снижения качества. Стеганография может быть использована для скрытия конфиденциальных данных, скрытой аутентификации для проверки подлинности видео или для скрытой передави информации.

Существует множество алгоритмов стеганографии для видеофайлов, которые можно разделить на несколько категорий: алгоритмы на основе LSB (Least Significant Bit), алгоритмы на основе DCT (Discrete Cosine Transform) и алгоритмы на основе преобразования Фурье. Методы простого замещения LSB изменяет младшие биты пикселей видеокадра для встраивания информации. Такие алгоритмы просты в реализации, однако отличаются низкой стойкостью к атакам и заметным снижением качества видео при большом объеме внедряемого сообщения. Метод дифференциальной модуляции LSB использует разницу между значениями соседних пикселей для встраивания информации. Отличается более высокой стойкостью в сравнении с простым замещением LSB. Метод встраивания в коэффициенты DCT использует коэффициенты DCT (дискретного косинусного преобразования) видеокадров для встраивания информации. Метод с использованием квантовых таблиц DCT модифицирует квантовые таблицы DCT для встраивания информации. Оба метода на основе DCT незначительно снижаю качество видео. Алгоритмы на основе преобразования Фурье более сложны в реализации по сравнению с алгоритмами LSB и DCT. Преобразования Фурье представляют собой разложение сигнала на его составляющие частоты, таким образом алгоритмы на основе таких преображений требуют больших вычислений и чувствительных к шуму [1].

Стеганографические методы можно разделить на две категории в зависимости от того, в каком виде используется видео: в исходном или сжатом виде. При разработке стеганографических методов для видеофайлов в сжатом виде необходимо учитывать особенности кодеков, которые используются для сжатия видео. Сжатые видео занима-

ют меньше места в памяти по сравнению с исходным вариантом, и встраивание сообщение происходит во время или после сжатия видео.

H.264 (также известный как AVC) – это стандарт сжатия видео, который использует алгоритм сжатия с межкадровым предсказанием, который кодирует изменения между кадрами, что позволяет значительно уменьшить размер видеофайла. H.264 использует ключевые I-кадры, которые не зависят от других кадров и содержат полную информацию, P-кадры для предсказания изменений в сравнении с предыдущими кадрами (они содержат только информацию о различиях между предыдущим кадром и самим собой) и B-кадры, которые используются для предсказания изменений как относительно предыдущих, так и последующих кадров.

Стеганографические алгоритмы, работающие с H.264, могут быть очень эффективными для скрытия информации. Это связано с тем, что H.264 основан на дискретном косинусном преобразовании, которое преобразует видеоданные в частотную область. Как правило, секретное сообщение встраивается в коэффициенты DCT яркости ключевого I-кадра [2]. В P-кадрах вектор движения кодируется для каждого макроблока на основе предыдущих кадров, для дальнейшей работы алгоритма. Вектор движения широко используется и для встраивания секретного сообщения. Можно воспользоваться одним из двух подходов: модификация вектора движения и модификация фазового ушла вектора движения [3].

H.265 (также известный как HEVC) – это стандарт сжатия видео, который был разработан для достижения более высокой степени сжатия, чем H.264. Он использует ряд новых технологий, таких как кодирование с использованием блоков большего размера, предсказание внутрикадрового кодирования и адаптивное кодирование энтропии, для достижения более высокой эффективности сжатия.

H.265 имеет ряд характеристик, которые могут быть использованы для встраивания скрытых данных. Однако, как и в случае с H.264, эффективность внедрения скрытых данных в видео с использованием H.265 может зависеть от ряда факторов, таких как качество видео и требования к скрытой информации. H.265 использует более крупные блоки предсказания (до 64x64 пикселей) по сравнению с H.264 (до 16x16 пикселей). Это увеличивает количество доступных данных для встраивания, что позволяет стеганографическим методам скрывать более объемные сообщения. Различные методы предсказания, такие как медианное предсказание и предсказание с использованием градиента, могут быть использованы для маскировки скрытых данных.

AV1 основан на алгоритме сжатия с потерями, который использует различные методы для уменьшения размера видеофайла без значительного снижения качества изображения. AV1 использует адаптивное квантование, которое позволяет ему эффективно распределять биты на блоки в зависимости от их содержимого. Это помогает сохранить детали и текстуры в сценах с высоким содержанием деталей, а также обеспечить лучшее сжатие для менее сложных сцен. Также AV1 использует различные преобразования сигналов, такие как дискретное косинусное преобразование и ортогональное преобразование Хаара для преобразования блоков изображения в частотную область перед их сжатием. При внедрении скрытого сообщения возможно использование внутренних углов предсказания [4].

Одним из способов внедрения секретного сообщения с использованием вышеперечисленных кодеков является использование внутрикадрого предсказания. Каждый кодек имеет свои особенности, которые могут влиять на выбор и эффективность стеганографического алгоритма. Для повышения эффективности и надежности стеганографии видео необходимо модифицировать алгоритмы, которые используются. Такие модификации могут быть направлены на увеличение емкости (максимального количества данных, которые могут быть скрыты в контейнере) и стойкости к атакам (уровень защиты скрытых данных к атакам).

ЛИТЕРАТУРА

1. Куликов Д.Л. Алгоритм стеганографии в видео с повышенной устойчивостью к искажениям // Новые информационные технологии в атоматизированных системах, №13. – 2010 – С. 303–305.

2. Goljan M. Searching for the Stego Key / M. Goljan, D. Soukal // Proc. SPIE, Electronic Imaging, Security, Steganography, and Watermarking of Multimedia Contents VI. – 2014. – P. 70–82.

3. Kunhoth, J., Subramanian, N., Al-Maadeed, S. Video steganography: recent advances and challenges // Multimed Tools Appl 82. –2023 – P. 41943–41985.

4. Catania L. Introducing AV1 Codec-Level Video Steganography // International Conference on Image Analysis and Processing. – Cham : Springer International Publishing, 2022. – P. 284–294.