ВЫБОР ИЗОБРАЖЕНИЯ ДЛЯ СТЕГАНОГРАФИЧЕСКОГО ВСТРАИВАНИЯ

С.А. СЕЙЕДИ, Н.Н. ИВАНОВ

Стеганография является одним из методом сокрытия информации. Стеганографические методы в изображениях стремятся максимизировать объем внедряемого сообщения при минимизации уровня искажений и обнаруживаемости сообщения в стего-изображении. Свободный выбор контейнера является особым преимуществом методов стеганографии по сравнению с другими методами сокрытия информации. До настоящего времени основное внимание в стеганографии было направлено на разработку новых методов внедрения секретного сообщения. Однако в конкуренцию с методами стеганографии вступают методы стегоанализа. Обоснованный выбор контейнера может существенным образом повлиять на результат, так как внедрение сообщения в разных контейнеры дает существенно различные результаты.

Для решения этой задачи, предлагается двухуровневая классификация изображений, основанная на выделении границ объектов и текстуры. На первом уровне критерием является количество пикселей, образующих грани объектов, на втором уровне площади текстурных областей. В обеих процедурах контейнер разделяется на квадратные блоки. Грани характеризуются дисперсией интенсивностей в блоке, текстурные блоки выделяются по превышению энтропии интенсивностей адаптивного порогового значения. Если изображение содержит достаточно много специфических деталей, таких, например, как грани объектов, то его можно рассматривать как потенциальный контейнер. Классификация предназначена для выбора контейнера отправителем в соответствии с его запросами.

Выбором подходящего контейнера отправитель может усилить действие применяемого стеганографического алгоритма в соответствие со своими предпочтениями не уменьшая стойкость стего-изображения к атакам.

ЭФФЕКТИВНЫЙ АЛГОРИТМ ФОРМИРОВАНИЯ ПРЕДСТАВИТЕЛЕЙ ОРБИТ ПРИ ДЕЙСТВИИ КВАДРАТА СИММЕТРИЧЕСКОЙ ГРУППЫ НА (0, 1)-МАТРИЦАХ

А.И. СЕРГЕЙ, В.А. ЛИПНИЦКИЙ

Актуальна задача классификации квадратных матриц порядка n с элементами 0 и 1, содержащих n единиц при действии независимых симметрических групп на строках и столбцах этих матриц. Для задач распознавания образов и помехоустойчивого кодирования важно иметь полный список матриц представителей получаемых классов.

Предлагается следующий быстрый алгоритм генерации представителей классов. Алгоритм состоит из двух этапов:

а) генерирование группы матриц, представляющих все орбиты;

б) просеивание построенной группы матриц с целью выбраковки дубликатов представителей классов.

Первый этап алгоритма выполняется следующим образом: строятся все матрицы, в которых суммы по строкам и по столбцам не убывают, а строки с одинаковой суммой упорядочены лексикографически. В полученных матрицах отсортируем группы столбцов с одинаковой суммой лексикографически и избавимся от повторов.

Второй этап алгоритма заключается в приведении каждой матрицы к единообразному виду путем перестановки строк и столбцов. Переберем перестановки столбцов, сохраняющие свойство неубывания сумм по столбцам. При фиксированной перестановке столбцов, строки достаточно отсортировать лексикографически.

Пользуясь полученными представителями классов, посчитаем количество классов с фиксированным рангом r. Прослеживается закономерность в количествах классов для рангов, близких к n. Так, для $r = n - 1$ при $n \geq 3$ имеется 3 класса, для $r = n - 2$ при $n \geq 6$ имеется 15 классов, что подтверждает известные вычисления. Установлено, что для $r = n - 3$ имеется 69 классов при $n \geq 9$ и для $r = n - 4$ имеется 342 класса при $n \geq 12$. Отсюда можно сделать предположение, что количество классов с фиксированным рангом начиная с некоторого момента перестает меняться.

ПРИМЕНЕНИЯ ГЕНЕРАТОРОВ КОНСТАНТ ДЛЯ ЗАЩИТЫ ЦИФРОВЫХ СХЕМ

В.В. СЕРГЕЙЧИК, А.А. ИВАНЮК

Схемная обфускация представляет собой методику защиты цифровых устройств от обратного проектирования. Одним из методов схемной обфускации цифровых устройств является внедрение генераторов констант (ГК). ГК — разновидность непрозрачных предикатов. ГК представляют собой схемы, генерирующие одно логическое значение постоянно. Сложность реализации ГК заключается в создании нераспознаваемых и неминимизируемых средством синтеза схем. Примером ГК может быть элемент памяти, в котором вход асинхронного сброса дополнительно соединен с выходом вентилем *and*. Некоторые применения ГК: вместо сигнальных источников ‘0’ и ‘1’ в схеме; мнимое объединение несвязанных узлов схемы мультиплексором (при подключении к селекторному входу ГК всегда будет выбираться один и тот же путь); создание обфусцированных вариантов основных логических вентилей с использованием ГК и мультиплексора. Второй способ применения был экспериментально изучен для FPGA на тестовых наборах комбинационных схем ISCAS-85 и последовательностных схем ITC-99 с использованием описанных выше примитивов ГК, которые внедрялись в участки, не входящие в критический путь. При этом синтезаторы (Xilinx xst 8.1 и Leonardo Spectrum 2007), во-первых, не смогли минимизировать ГК, во-вторых, сгенерировали неверную информацию о критическом пути (проложив путь через никогда не выбираемый маршрут в мультиплексоре с ГК). Дополнительная задержка, вносимая ГК, равна сумме задержек мультиплексора и двух проводящих линий. Таким образом, с помощью ГК можно не только усложнить анализ схемы, но и ввести в заблуждение атакующего относительно временных характеристик схемы. Кроме того, дополнительно ГК можно использовать для внедрения водяных знаков в конфигурируемые логические блоки FPGA.

ЭЛЕМЕНТЫ КРИПТОАНАЛИЗА БЛОЧНОГО АЛГОРИТМА ШИФРОВАНИЯ С ИСПОЛЬЗОВАНИЕМ ДИНАМИЧЕСКОГО ХАОСА

А.В. СИДОРЕНКО, Д. А. ЖУКОВЕЦ

Широкое распространение информационных технологий практически во всех сферах жизнедеятельности человека способствует появлению новых задач, связанных с обеспечением необходимой степени защиты информации.

Среди различных методов защиты информации и обеспечения ее целостности выделяются криптографические методы. Одним из перспективных направлений в современной криптографии является разработка алгоритмов шифрования на основе динамического хаоса [1]. Применение динамического хаоса для систем защиты информации обусловлено способностью с помощью хаотических отображений обеспечивать скрытость передачи зашифрованной информации и, прежде всего, в блочных шифрах. Детерминизм хаоса способствует шифрованию информации, а его случайность делает систему стойкой к вскрытию.