Министерство образования Республики Беларусь
Учреждение образования
Белорусский государственный университет
информатики и радиоэлектроники

УДК_____

Гордеенко
Илья, Сергеевич

Гибридные алгоритмы защиты полутоновых изображений

АВТОРЕФЕРАТ

на соискание степени магистра технических наук
по специальности 1-45 80 02 "Телекоммуникационные системы и компьютерные сети"

_____

Научный руководитель
Борискевич Анатолий Антонович
кандидат технических наук
доцент кафелры СиУТ

_____

Минск 2014

ВВЕДЕНИЕ

Общедоступность цифровой мультимедийной информации, а также ускоренный рост проводных и беспроводных коммуникационных технологий привели к тому, что проблема защиты данной информации вышла на первый план. В частности, задачи эффективного мультимедийного шифрования данных в последнее время получили больше внимания, как в академических, так и в промышленных кругах. Хотя шифрование всей мультимедийной информации, осуществляемое традиционной криптографией, дает удовлетворительный уровень безопасности, такой подход имеет несколько недостатков. Во-первых, вычислительные затраты, связанные с шифрованием всей мультимедийной информации зачастую высоки в связи с большим объемом данных. Во-вторых, операции шифрования и дешифрования добавляют еще один уровень сложности к системе. В большинстве случаев, необходимы дополнительные аппаратные или программные функции. Это особенно неблагоприятно в некоторых случаях, таких как мобильная связь и встраиваемые системы, где устройства (например, сотовые телефоны и портативное оборудование) испытывают дефицит ресурсов из-за ограниченного размера и энергопотребления. Следовательно, необходимо разработать эффективную и надежную мультимедийную технику шифрования.

При сравнении мультимедийных процессов сжатия и шифрования с точки зрения теории информации, оба могут в целом рассматриваться как процесс удаления избыточности, содержащейся во входных данных. Основное различие между ними состоит в том, что секретный ключ контролирует операции шифрования, в то время как все операции по сжатию осуществляются в соответствии с некоторыми стандартами. Основная идея нового подхода к шифрованию заключается в использовании нескольких параметров энтропийного кодирования в соответствии со случайной последовательности.

Совместное использование сжатия и шифрования имеет несколько преимуществ. Во-первых, данный подход использует структуру энтропийного кодера, что приводит к незначительной вычислительной сложности реализации в аппаратном или программном обеспечении. Во-вторых, шифрование не ухудшает степень сжатия в том смысле, что размер зашифрованного потока точно такой же, как и при стандартном сжатии. С точки зрения безопасности, предлагаемый алгоритм является устойчивым к различным типам криптоатак.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Цель исследования состоит в разработке алгоритма сжатия на основе энтропийного кодера и предсказания изображения, а также изучение возможности интеграции алгоритма сжатия с хаотическим генератором.

Для достижения цели необходимо решить следующие задачи:

1) анализ предсказателей изображений;

2) выбор оптимального предсказателя изображения;

3) анализ алгоритмов энтропийного кодирования;

4) выбор алгоритма энтропийного кодирования;

5) анализ хаотических генераторов;

6) выбор хаотического генератора;

7) программная реализация алгоритма предсказания изображения с использованием различных предсказателей и алгоритмов энтропийного кодирования,

8) программная реализация хаотического генератора;

9) программная реализация шифрования RC4

10) интеграция сжатия и шифрования с помощью хаотического генератора;

11) оценка быстродействия алгоритма сжатия совместно с алгоритмом шифрования RC4 и гибридного алгоритма сжатия с использованием хаотического генератора;

В исследовании решается изучается возможность согласования сжатия и шифрования в пространственной области.

Проанализированы и реализованы девять вариантов алгоритма сжатия и шифрования полутонового изображения в пространственной области:

– алгоритм работы адаптивного энтропийного экспоненциально- го кодера Голомба с предсказателями Loco1, Paeth, Gap совместно с генератором хаотической последовательности.

– алгоритм работы энтропийного кодера Хаффмана с предсказ- ателями Loco1, Paeth, Gap совместно с генератором хаотической последовательности.

– алгоритм работы адаптивного энтропийного кодера Голомба-Райса с предсказателями Loco1, Paeth, Gap совместно с поточным шифром RC4.

Произведен сравнительный анализ результатов работы алгоритмов сжатия и оценка быстродействия гибридных алгоритмов.

Программная реализация алгоритмов сжатия и шифрования изображений осуществлена при помощи языка программирования C++ и стандартной графической библиотеки MFC.

Результаты работы представлены на конференции БГУИР в 2013 году.

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

Во введении обоснована актуальность темы диссертации, формулируются цель и основные задачи исследуемой работы.

В первой главе рассматриваются общая схема алгоритма предиктивного кодирования. Проводится анализ предсказателей изображений Paeth, Loco1 и Gap. Приведены формулы расчёта предсказателей.

В п.1.6 описан алгоритм вычисления разностного изображения.

В п.1.7 описан алгоритм преобразования разностного изображения к целочисленному положительному виду.

В п. 1.8 рассматриваются следующие методы анализа эффективности предсказателей изображений: минимальная среднеквадратическая ошибка (MMSE), минимальная средняя абсолютная ошибка (MMAE), энтропия разностного изображения.

В п.1.9 приводятся результаты расчёта эффективности предсказателей изображения.

Установлено, что для стандартных изображений предсказатель Gap даёт наилучший результат. Для изображений отличающийся классом видно, что предсказатель Loco даёт наилучший результат при использовании кодера Голомба – Райса, в частности для медицинских изображений и изображений отпечатков пальцев. При этом стоит заметить, что средний коэффициент для предсказателя Gap не на много меньше чем для Loco, в частности для стандартных и космических изображений коэффициент полученный при использовании предсказателя Gap даже превосходит результаты предсказателя Loco1.

Во второй главе рассматриваются три универсальных компрессора: экспоненциальный кодер Голомба, адаптивный кодер Голомба-Райса, кодер Хаффмана.

В п.2.4 приведены результаты моделирования алгоритмов с предсказанием. В качестве исходных данных использовались изображения с различными энтропией и размерами.

Установлено, что максимальный коэффициент сжатия получается при сочетании предиктора Gap и адаптивного кода Голомба-Райса. Минимальный коэффициент получается при нескольких сочетаниях алгоритмов. Однако стоит заметить, что RAR архиватор сжимает на уровне нижних значений коэффициентов сжатия, ZIP архиватор сжимает данные намного хуже. Тем самым можно утверждать, что найдено несколько хороших алгоритмов, значительно опережающих по коэффициенту сжатия универсальные алгоритмы сжатия данных.

В третьей главе рассматривается обобщенный алгоритм сжатия и шифрования, а также предлагается способ одновременного шифрования во

время сжатия изображения с использованием генератора псевдослучайной хаотической последовательности.

В п.3.1 рассматриваются три генератора псевдослучайной хаотической последовательности: Логистический, PWAM1 и Sine. В результате анализа различных параметров генераторов установлено, что хаотическая последовательность, генерируемая генератором PWAM1, обладает наилучшими свойствами и успешно прошла тестирование тестами NIST.

В п.3.2 приведён алгоритм RC4, который использован для оценки быстродействия гибридного алгоритма сжатия с шифрованием.

В п.3.3 описывается алгоритм сжатия Голомба-Райса с шифрованием, приводится пример кодирования последовательности алгоритмом сжатия Голомба-Райса с шифрованием. Суть алгоритма состоит в следующем:

1) генератор псевдослучайной последовательности, выдавая ноль или единицу, определяет какой кодировкой воспользоваться для кодирования текущего символа;

2) декодирование битового потока сгенерированного предложенным алгоритмом становится невозможным без правильно сгенерированной псевдослучайной последовательности и криптостойкость алгоритма будет определяться криптостойкостью генератора псевдослучайной последовательности.

В п.3.4 производится оценка быстродействия гибридного алгоритма сжития Голомба-Райса с шифрованием.

Установлено, что при маленьком размере изображения комплексные алгоритмы выигрывают по абсолютной величине почти в два раза. При среднем размере изображения результат практически одинаков. При большом размере изображения комплексные алгоритмы проигрывают по абсолютной величине почти в два раза.

Исходя из результатов, можно сделать вывод, что совместные алгоритмы можно успешно применять для передачи видео потоков в режиме онлайн, так как при частоте кадров 25 Гц, время на обработку одного кадра равно 40мс. Таким образом, около 20мс приведённый алгоритм оставляет на помехоустойчивое кодирование, что вполне достаточно.

Из результатов моделирования следует, что разработанный алгоритм является эффективным как по коэффициенту сжатия, так и по быстродействию.

В четвертой главе изображен пользовательский интерфейс программы и приведены графические схемы работы программы.

В заключении сформулированы основные результаты, полученные в диссертационной работе.

В приложении предоставлен графический материал использованный для презентации во время защиты.

ЗАКЛЮЧЕНИЕ

Разработан быстрый блочный алгоритм сжатия полутоновых изображений без потерь, основанный на локальном предсказании изображений и адаптивном энтропийном кодировании. Рассмотрено три вида предсказателей и три вида энропийного кодирования. Данный алгоритм позволяет повысить коэффициент сжатия при сохранения высокого быстродействия за счёт выбора предсказателя и энтропийного кодера.

Предложен способ объединения алгоритмов сжатия и шифрования, основанный на псевдослучайном выборе типа кодирования для сжатия символов источника информации. Псевдослучайная последовательность формируется при помощи бинарного хаотического генератора. Данный способ обладает высокой криптографической стойкостью против стандартных методов криптографических атак за счёт формирования псевдослучайной структуры сжатого битового потока. Пространство секретных ключей определяется типом и разрядностью ключевых параметров хаотического генератора.

Разработана программная реализация алгоритма сжатия с и без шифрования на языке программирования C++.

Установлено что наибольшее влияние на коэффициент сжатия оказывает выбор предсказателя. Определено, что быстродействие меньше зависит от вычислительной сложности предсказателей и больше зависит от выбора энтропийного кодера.

СПИСОК ОПУБЛИКОВАННЫХ РАБОТ

1-А. - Гордеенко, Анализ эффективности предсказателей изображения Loco1, Paeth, Gap / 49-я научно-техническая конференция аспирантов, магистрантов и студентов БГУИР, 6-10 мая 2013г., Минск: БГУИР.