Условный доступ к мультимедийным данным с разным качеством основан на декомпозиции контента, представлении его в виде множества пакетов, селективном или полном шифровании пакетов. Шифрование пакетов может быть произведено несколькими способами. Простейший способ заключается в шифровании каждого пакета независимыми ключами. При этом множество ключей декоррелированно, что не дает возможности осуществить коалиционную атаку на ключи. Однако в этом случае лицензия, выдаваемая пользователю, должна содержать множество ключей, необходимых для расшифрования контента с заданным качеством. Количество передаваемых ключей зависит от параметров декомпозиции контента и предоставляемого уровня качества. Другим подходом к решению проблемы является использование иерархии ключей. При использовании иерархии ключей лицензия содержит только один ключ, необходимый для расшифрования контента. Нижестоящие в иерархии ключи определяются через одностороннюю хэш-функцию. Недостатком применения иерархии ключей является их подверженность коалиционным атакам при более двух типах декомпозиции и отсутствии дополнительных мер защиты.

Для организации защищенного от коалиционных атак условного доступа к мультимедийному контенту предлагается система условного доступа, основанная на модифицированной структуре иерархических ключей. Защита от коалиционных атак осуществляется за счет введения дополнительных защитных субключей и основывается на дополнении или замещении исходной иерархии ключей защищенной иерархией. При этом предлагаемая система имеет режим частичной защиты с запрещением перехода к высшим уровням качества и режим полной защиты от коалиционных атак. Режим частичной защиты обеспечивает большее быстродействие за счет незначительного увеличения структуры ключа. Данный режим может быть использован для контента с большим количеством типов и уровней декомпозиции. Режим полной защиты полностью предотвращает коалиционные атаки на секретные ключи, но требует большее количество защитных субключей и имеет меньшее быстродействие. Предлагаемая система поддерживает как полное, так и селективное шифрование контента в зависимости от требований к быстродействию и деградации качества при восстановлении контента без вышестоящих в иерархии ключей.

Гибкость разработанной системы дает возможность использовать ее для широкого спектра задач, направленных на организацию условного доступа к мультимедийному контенту в глобальной сети.

АЛГОРИТМ ГЕНЕРАЦИИ ХАОТИЧЕСКИХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ С УЛУЧШЕННЫМИ КРИПТОГРАФИЧЕСКИМИ ХАРАКТЕРИСТИКАМИ

А.А. БОРИСКЕВИЧ, Д.М. ШУТ

Генерация псевдослучайных последовательностей с хорошими криптографическими характеристиками является одной из важнейших задач в области защиты информации. Одной из причин использования цифровых хаотических систем для улучшения качества генераторов является простота реализации и тесная взаимосвязь между хаотическими (эргодичность, высокая чувствительность к начальным условиям/ управляющему параметру, детерминированная динамика и структурная сложность) и криптографическими свойствами (перемешивание, рассеяние, детерминированная псевдослучайность, алгоритмическая сложность).

Предложен алгоритм генерации бинарных хаотических последовательностей, основанный на использовании модели детерминированного хаоса, генерации начальных значений (сеансовых ключей) из секретного ключа, генерации последовательности целых и вещественных хаотических значений, перемешивании вещественных хаотических значений с помощью целочисленных хаотических значений, бинаризация перемешанных хаотических значений.

Разработанный алгоритм позволяет формировать бинарные и вещественные хаотические последовательности с улучшенными криптографическими свойствами (баланс {0, 1}, большая длина цикла, высокая линейная сложность, и т.п.) за счет увеличения пространства ключей (начальное значение хаотической переменной, управляющий параметр и параметр безопасности) и использования операции перемешивания.

Проведена оценка качества сгенерированных последовательностей с использованием пакета из 15 статистических тестов NIST, целью которой было определение и подтверждение случайного характера бинарных хаотических последовательностей.

АЛГОРИТМ ОБНАРУЖЕНИЯ НИЗКОКОНТРАСТНЫХ ОБЪЕКТОВ В ВИДЕОПОСЛЕДОВАТЕЛЬНОСТИ НА ОСНОВЕ ИЗБЫТОЧНОГО ДИСКРЕТНОГО ВЕЙВЛЕТ-ПРЕОБРАЗОВАНИЯ

И.А. БОРИСКЕВИЧ

Для обнаружения низкоконтрасных объектов на ИК-изображениях требуется выделить пиксели целей на фоновом изображении в условиях низкого отношения сигнал/шум. Известные алгоритмы не позволяют обнаружить цели с заданной степенью достоверности. В связи с этим предложен алгоритм, основанный на вычислении избыточного дискретного вейвлет-преобразования, попиксельной и локальной обработке матриц аппроксимирующих и/или детализирующих вейвлет-коэффициентов, формировании интегрального вейвлет-изображения с близкой к требуемой форме гистограммы, бинаризации и бинарной морфологической операции наращивания. Он позволяет обнаружить низкоконтрастные объекты за счет использования свойств избыточного дискретного вейвлет-преобразования с определенным уровнем разложения, оптимальных вейвлет-функций и выбранного правила объединения вейвлет-матриц. Избыточное дискретное вейвлет-преобразование производит локализацию компонент исходного изображения в пространственно-частотной области с сохранением его энергии, что гарантирует отсутствие искажения значимых деталей и позволяет произвести анализ динамики изменения локальных статистических параметров изображения на разных уровнях.

Оценка эффективности предложенного алгоритма была произведена с использованием ROC-кривых (Receiver Operating Characteristic), позволяющих оценить соотношение вероятности правильного обнаружения и ложной тревоги. Из анализа кривых следует, что предложенный алгоритм увеличивает вероятность правильного обнаружения на величину до 50% по сравнению с известными алгоритмами за счет большей устойчивости к изменению размеров целей и инвариантности к сдвигу. Моделирование проведено в среде Matlab для пяти уровней разложения и четырех вейвлет-функций. Последовательность тестовых изображений содержит низкоконтрастные малоподвижные объекты размером 3–25 пикселей, искаженные аддитивным гауссовским шумом.