шифрованием данных, негативно влияют на характеристики сети: время задержки, полезную пропускную способность, время конвергенции и другие. Поэтому важно правильно выбрать необходимые и достаточные средства защиты для конкретной сети.

МОДЕЛЬ НЕРАВНОМЕРНОГО КРИПТОГРАФИЧЕСКОГО КОДИРОВАНИЯ МНОГОРАКУРСНЫХ ИЗОБРАЖЕНИЙ НА ОСНОВЕ МАТРИЦЫ ПЕРЕКРЫТИЯ

В.Ю. ЦВЕТКОВ, К.С.Ш. АЛЬ-САФФАР, А.Д.К. АЛЬ-ГЕЙЗИ, М.Д.А. АЛЬ-ДЖЕБНАВЕ

Развитие систем передачи многоракурсных изображений, формируемых камерами, установленными на подвижных объектах, требует разработки соответствующих систем защиты. В связи с большим объемом видеоинформации, формируемой и передаваемой в таких системах, актуальной задачей является использование для ее защиты неравномерного криптографического кодирования, выбирающего сложность шифра с учетом важности защищаемой информации. Для решения данной задачи предлагается использовать модель неравномерного криптографического кодирования многоракурсных изображений на основе матрицы перекрытия. Элементами матрицы перекрытия являются фрагменты многоракурсного изображения, относящиеся к определенному ракурсу — оригинальные (главная диагональ), и фрагменты, присутствующие в разных ракурсах — перекрывающиеся (остальные элементы). Элементы главной диагонали сжимаются и передаются независимо друг от друга. Они должны шифроваться наиболее стойким шифром. Остальные элементы являются избыточными. Их сжатие основано на компенсации движения, что предполагает формирование опорных изображений и использование их для предсказания остальных. Из-за перекрытия опорные изображения могут быть равномерно распределены по различным ракурсам и переданы по различным каналам, что усложняет процедуру несанкционированного доступа к ним. В этой связи для шифрования опорных изображений может использоваться менее стойкий шифр по сравнению с оригинальными. Несовершенство методов предсказания приводит к различию прогнозируемых и прогнозных изображений, что требует передачи ошибки предсказания для каждого ракурса. Данная видеоинформация имеет, как правило, малый динамический диапазон и может кодироваться наименее стойким шифром.

СКРЫТНАЯ ПЕРЕДАЧА ДАННЫХ В ИЗОБРАЖЕНИЯХ С ИСПОЛЬЗОВАНИЕМ МАНИПУЛЯЦИИ РАЗМЕРАМИ СЕГМЕНТОВ

В.Ю. ЦВЕТКОВ, О.М. АЛЬМИЯХИ, В.К. КОНОПЕЛЬКО

Предлагается метод скрытной передачи данных в изображениях на основе манипуляции доминирующим размером сегментов. Сущность метода состоит в изменении наиболее часто встречающегося на изображении размера сегментов в соответствии со значениями бит скрываемого сообщения. Алгоритм реализации данного метода состоит из следующих шагов: сегментация изображения; построение гистограммы размеров сегментов; определение локальных экстремумов гистограммы; определение правого доминирующего локального экстремума гистограммы; нормализация гистограммы вблизи локального экстремума (выравнивание размеров сегментов, близких к доминирующему размеру); локализация сегментов доминирующего размера; согласование объема скрываемых данных с числом локализованных сегментов; определение порядка выборки сегментов для манипуляции; манипуляция размеров сегментов в соответствии со значениями бит скрываемого сообщения. Для исключения необходимости последующей обработки границ сегментов, размеры которых в результате манипуляции уменьшаются, предлагается использовать только увеличение размеров сегментов при сокрытии единичных бит данных и сохранение размеров при сокрытии нулевых бит данных.

Алгоритм извлечения данных из изображения включает большинство операций алгоритма погружения. Его особенностью является локализация двойного доминирующего локального экстремума. Для повышения устойчивости работы декодера предлагается использовать скремблирование скрываемых данных. Метод обеспечивает устойчивость к проективным преобразованиям, зашумлению, изменению яркости и контраста изображения.

СИСТЕМА ОБНАРУЖЕНИЯ ВТОРЖЕНИЯ В САМООРГАНИЗУЮЩУЮСЯ МОБИЛЬНУЮ СЕТЬ НА ОСНОВЕ ПАТТЕРНОВ МОБИЛЬНОСТИ

А.А. ПОДЛУЦКИЙ, В.Ю. ЦВЕТКОВ

В настоящее время с развитием теории беспроводных самоорганизующихся сетей (Ad-Hoc сетей) все большее внимание уделяется вопросам безопасности. Это связано с тем, что в основе функционирования таких сетей лежит принцип тесного и открытого взаимодействия узлов сети. При этом сеть часто должна предоставлять доступ предварительно неизвестным узлам, особенно, когда узлы проходят через нее транзитом. Все это приводит к тому, что внедрение вредоносных узлов становится сравнительно легкой задачей. Для выявления таких узлов предлагается использовать систему обнаружения вторжения (intrusion detection system — IDS), основанную на составлении уровня доверия к узлам при помощи изучения их характера движения и сопоставления полученной информации с заранее созданными паттернами мобильности. Паттерны мобильности могут содержать информацию о допустимых скоростях движения, изменениях направления, ускорениях и т.д. Использование таких систем выявления аномального поведения наряду с традиционными методами авторизации узлов позволит существенно повысить безопасность беспроводных безинфраструктурных мобильных сетей.

ЗАЩИТА ДАННЫХ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА В БОРТОВОЙ ПАМЯТИ БЕСПИЛОТНОГО ЛЕТАТЕЛЬНОГО АППАРАТА НА ОСНОВЕ ДЕСТРУКТУРИЗАЦИИ

А.А ЖУРАВЛЕВ, В.Ю. ЦВЕТКОВ, Ф.А.-К.М. АЛЬ ХЕЛЛИ, М.Х. САЛЕК

Рассматривается проблема защиты видеоданных и телеметрии, записанных в бортовую память беспилотного летательного аппарата (БЛА) во время полета, от несанкционированного доступа в случае потери БЛА. Наиболее эффективным решением данной проблемы является шифрование всей информации, которая записывается в бортовую память. Однако, данные телеметрии, формируемые в процессе полета БЛА, содержат априорную информацию, которая часто повторяется и может быть легко восстановлена. В первую очередь это GPS-координаты точки приземления и траектории полета БЛА, которые записываются в бортовую память БЛА вместе с каждым кадром видеоданных. При скорости БЛА 25–30 м/с, точности измерения GPS-координат 20 м и частоте видеокадров 25–30 Гц одни и те же значения GPS-координат соответствуют 16–25 кадрам видеоданных. Кроме GPS-координат телеметрия содержит десятки других медленно изменяющихся параметров относительно частоты кадров и перемещения БЛА. Эта информация может эффективно использоваться при дешифровании. Поэтому в качестве дополнительного к зашифрованию средства, повышающего защищенность информации в бортовой памяти БЛА от несанкционированного доступа, предлагается использовать ее случайную или хаотическую деструктуризацию, которая предполагает изменение расположения данных в памяти, а также разрядов в кодовом представлении чисел по соответствующему закону. Деструктуризация, в отличие от сжатия, позволяет