считывателя к другому компьютеру. Это позволяет произвести настройку или конфигурирование считывателя на одном компьютере, а эксплуатировать – на другом компьютере. Используемое программно-аппаратное оборудование соответствовало основному действующему стандарту ISO/IEC 18000-2:2009. Дистанция регистрации обычно составляла 10 ~ 50 мм. Оборудование близкого чтения недорого, но сами метки являются относительно дорогими и без перспектив удешевления из-за конструктивных особенностей их изготовления.

ИСПОЛЬЗОВАНИЕ ВЕРОЯТНОСТНЫХ СТРУКТУР ПРИ РАБОТЕ С БОЛЬШИМИ ОБЪЕМАМИ ДАННЫХ

И.Е. Закревский

Операции над большими массивами данных являются неотъемлемой частью ежедневной работы. Растут базы данных, что сказывается на скорости работы средств защиты информации, таких как средства аутентификации, DLP системы, анализаторы трафика и т.д. Одним из путей решения проблем скорости доступа является использование вероятностных структур данных, в частности – фильтр Блума.

Фильтр Блума – это вероятностная структура данных, позволяющая хранить и проверять принадлежность элемента к множеству [1]. В фильтре Блума возможны ложноположительные срабатывания. Фильтр Блума представляет собой битовый массив из m бит, которые по умолчанию обнулены. Далее, пользователю необходимо определить k независимых хеш-функций, которые будут преобразовывать массив входных данных произвольной длины в битовую строку фиксированной длины m достаточно равномерным способом. Процент ложноположительных может быть уменьшен увеличением размера массива m и/или числа хеш-функций k [2].

В данной работе был реализован фильтр Блума ($k = 3$, $m = 109$) и использован для определения необходимости вызова удаленной БД. Использование фильтра Блума в качестве структуры данных для хранения информации о наличии элемента в БД позволило сократить на 77 % используемую память по сравнению с хеш-таблицами, также незначительно уменьшило время на добавление состояния новых элементов в множество (> 5 %).

Литература

1. Bloom, B.H. Space/time trade-offs in hash coding with allowable errors.
2. Dillinger, P.C. Fast and Accurate Bitstate Verification for SPIN.

РАЗРАБОТКА ПРИЛОЖЕНИЙ ДЛЯ БЕЗОПАСНЫХ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ НА ОСНОВЕ ГОМОМОРФНОЙ КРИПТОГРАФИИ И ОЦЕНКА ИХ ЭФФЕКТИВНОСТИ

М.А. Кадан

С внедрением повсеместного использования облачных технологий остро встает вопрос сохранности данных и их безопасной обработки в облачных хранилищах. Разумным решением проблемы обеспечения конфиденциальности данных может служить шифрование всех приватных данных перед передачей в облако и обеспечение выполнения операций над зашифрованными данными, без их предварительного дешифрования, известное как гомоморфное шифрование [1].

Предметом доклада является применение гомоморфного шифрования в реализации безопасных мобильных приложений для облачных вычислений. Рассматривается задача определения требований к безопасности использования облачных хранилищ данных и подходов к проведению безопасных вычислений над данными облачного хранилища с использованием методов гомоморфного шифрования [2].

На основе теоретических принципов гомоморфного шифрования обоснован, спроектирован и реализован модуль для обеспечения возможности безопасного хранения и обработки данных в облачных структурах, не имеющий аналогов для решения задач данного рода на платформе iOS. Исследована эффективность использования метода гомоморфного шифрования в зависимости от максимальной длины операндов и ключа шифрования, а также исследована производительность модуля с использованием приложения на языке Swift.

Литература

1. Craig Gentry, Fully homomorphic encryption using ideal lattices, Symposium on the Theory of Computing (STOC). – 2009. – P. 169–178.

2. Кадан, М.А. Безопасные вычисления с использованием гомоморфной криптографии для облачных хранилищ данных / М.А. Кадан, М.А. Макарычев // Современные информационные технологии и ИТ-образование. 2016. – Т. 12, № 3. – С.43–49.

ПОДТВЕРЖДЕНИЕ ПОДЛИННОСТИ ЦИФРОВЫХ ФОТОГРАФИЙ НА ОСНОВЕ РАЗЛИЧИЙ JPEG-ФОРМАТОВ

А.М. Кадан, П.С. Каспер, А.И. Лазарь, Н.А. Радевич, Е.А. Шишкин

Современные цифровые фотокамеры и фотографии, полученные с их помощью, являются носителями информации, значимой для компьютерной технической экспертизы.

Целью данной работы является исследование особенностей формата JPEG, связанных с особенностями программно-технической реализации цифровых фотокамер различных производителей, и формирование наборов признаков для применения методов машинного обучения в задачах классификации цифровых фотокамер (брэнд / модель) на примере задачи определения подлинности цифровых изображений в JPEG-формате.

Согласно требованиям стандарта ISO/IEC 10918-1, JPEG-файл содержит последовательность маркеров, каждый из которых начинается с байта 0xFF.. В то же время в структуре JPEG-формата у различных производителей отличается типы используемых маркеров, количество вхождений маркеров одного типа в структуру файла, длина блока кода, связанного с такими маркерами, порядок появления маркеров в JPEG-файле и другие характеристики, также связанные с маркерами. Различия в использовании маркеров наблюдаются не только в файлах различных производителей фотоаппаратуры, но и для различных моделей одного и того же производителя, а также и для одних и тех же моделей при выборе различных режимов фотосъемки. Использование графического редактора также изменяет структуру исходного JPEG-файла, что позволит идентифицировать программное средство, с помощью которого была нарушена подлинность исходного изображения.

Сказанное выше позволяет выдвинуть гипотезу, что анализ структуры JPEG-формата цифрового изображения позволит получить ответы на вопросы: является ли данное цифровое изображение оригинальным, не подвергалось ли оно редактированию в графическом редакторе; определить бренд-модель цифровой фотокамеры, которой сделано данное изображение.

В ходе выполнения работы была сформирована база, включающая более 1500 различных комбинаций бренд-модель и более 25000 оригинальных цифровых фотографий, ставшая основой для наборов признаков, использованных в методах машинного обучения, положенных в основу приложения для проверки подлинности цифровых изображений.

СЕРВИС ДЛЯ ПРОВЕРКИ ПОДЛИННОСТИ ЦИФРОВЫХ ФОТОГРАФИЙ

А.М. Кадан, П.С. Каспер, А.И. Лазарь, Н.А. Радевич, Д.Ю. Сенько, Е.А. Шишкин

Цифровые фотографии стали неотъемлемой частью информационного обеспечения различных процессов, но широкая доступность инструментов для редактирования изображений зачастую ставит под сомнение их подлинность. Современные цифровые фотокамеры и фотографии, полученные с их помощью, являются носителями криминалистически значимой информации, а количество различных способов мошенничества в сфере ИТ постоянно растет, будучи измененными, такие фотографии уже не будут нести достоверную информацию. Поэтому актуальной, и не только для специалистов в области компьютерной технической экспертизы, является задача обеспечения возможности подтверждения подлинности цифровых изображений. Подобные задачи актуальны, к примеру, в финансовых сферах, страховом деле, информационной безопасности, защите информации и криминалистике.

Под «подтверждением подлинности» будем понимать возможность определения бренда цифровой камеры и ее модели. Либо определение класса программного средства, с помощью которого было изменено оригинальное цифровое изображение.