

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 (бренд / 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.