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.

Целью данной работы является представление клиент-серверной системы, учитывающей особенности реализации формата JPEG, связанные с программно-технической реализацией цифровых фотокамер различных брендов и моделей, работа которой основана на применении методов машинного обучения для решения задачи определения цифровой фотокамеры (брэнд / модель), которой было сделано подлинное изображение, или определения графического редактора, которым были внесены изменения.

Сервис проверки подлинности цифровых изображений разработан и функционирует как локальное клиент-серверное приложение, так как передавать в локальную сеть, а тем более в сеть Интернет, криминалистически значимую информацию недопустимо. Сервис позволяет определять лишь подлинность изображений JPEG-формата, а сам процесс определения подлинности основан на алгоритмах классификации: построения дерева принятий решений и методе k ближайших соседей. В настоящее время база сервиса содержит информацию о 48 брендах (производителях цифровых фотокамер) и более чем 650 моделях.

СИСТЕМА SSO В ИНТЕГРИРОВАННОЙ СЕТИ

А.О. Качанова

Современная тенденция в области аутентификации является использование технологии единого входа (англ. Single Sign-On). Это удачный компромисс между безопасностью доступа к приложениям и удобством работы пользователя. Идея этой технологии заключается в обеспечении единой аутентификации для всех информационных систем организации, которые с точки зрения доступа являются разнородными и никак не интегрированы между собой или с общей службой каталогов. Кроме того, подобное решение повышает уровень информационной безопасности в части парольной политики. Областью практического применения данного исследования являются компании, которые имеют многочисленные внутренние подсистемы.

В докладе рассматривается система, использующая API технологию с использованием языка JSON, что позволяет обеспечить надежную политику безопасности, повышенную безопасность всех ресурсов предприятия, снизить вероятность возникновения критических ошибок, упростить процесс аутентификации пользователя в интегрированной сети. Система использует дополнительную биометрическую процедуру аутентификации.

Литература

1. Bashir, K., Asif, S. Important Considerations for Single Sign-On Solution. International Journal of Multidisciplinary Sciences and Engineering, 2010.

2. Bishop, M. Introduction to Computer Security. Boston: Pearson Education, 2005

АНАЛИЗ РЕЧЕВОЙ ИНФОРМАЦИИ КАК ЭТАП МНОГОФАКТОРНОЙ АУТЕНТИФИКАЦИИ В СЕТИ ИНТЕРНЕТ

Е.В. Кисель, А.В. Курочкин

В настоящее время значительное внимание уделяется задаче идентификации и аутентификации личности на основании одного или нескольких биометрических признаков. Одним из перспективных направлений в биометрической идентификации и аутентификации является распознавание речевой информации. Существенным преимуществом использования голоса в качестве одного из факторов аутентификации является отсутствие необходимости в сложном специализированном оборудовании – для записи образца голоса можно использовать обычный микрофон. Распознавание речевой информации может использоваться в качестве одного из факторов при проведении многофакторной аутентификации. В значительной степени многофакторная аутентификация может применяться для обеспечения безопасности при доступе на различные интернет-ресурсы. В данном контексте большой значимостью обладает задача автоматизированного распознавания речи в реальном времени в рамках проведения многофакторной аутентификации на веб-сайт. Пользователю предлагается, в качестве одного из этапов аутентификации для входа на защищенную зону веб-сайта, произнести заранее записанный пароль, который в дальнейшем сверяется с эталоном во внутренней базе данных; на основании результата сверки принимается решение о подтверждении или отклонении