Капшук О.А.
УНК "ИПСА" НТУУ "КПИ", Киев, Украина

Методы и средства защиты от спуфинга в биометрических системах контроля и управления доступом с использованием технологии распознавания лиц

Биометрические технологии идентификации (ТБИ) с использованием для распознавания изображения лица составляют примерно 11,4% мирового рынка биометрических систем и являются одним из самых быстро развивающихся направлений в биометрической индустрии [1].

Основная проблема всех ТБИ заключается в том, что результаты идентификации человека носят вероятностный характер и зависят от многих факторов. Биометрические системы контроля и управления доступом (СКУД), использующие ТБИ, уязвимы к атакам на различных стадиях обработки информации. Чаще всего системы подвергаются спуфингу (от англ. spoofing), т. е. обману с помощью предъявления сенсорам системы не самого пользователя, а фотографий его лица, муляжей отпечатков пальцев, заранее записанных звуков, видео данных и т. п. Спуфинг-атаки на этапе ввода данных наиболее опасны, так как злоумышленник непосредственно имеет контакт с сенсорами системы и невозможно использовать криптографические и другие методы защиты.

В настоящее время технологии распознавания лиц широко применяются в различных биометрических СКУД компаний, а также во многих моделях мобильных компьютеров. Например, компании Toshiba, ASUS, Lenovo в своих ноутбуках используют технологию Face Recognition позволяющую с помощью встроенной Web-камеры ввести один раз изображение лица в компьютер, а затем использовать лицо в качестве уникального пароля для получения доступа к системе. Программа Lenovo VeriFace позволяет, в случае попытки доступа к компьютеру лица, не соответствующего оригиналу, сделать снимок и записать время попытки несанкционированного доступа в журнале VeriFace. Аналогично работает и программа ASUS SmartLogon. По данным, приведенным в [2], 2D-технология Face Recognition неустойчива к спуфингу с использованием 2D-изображений и нуждается в усовершенствовании алгоритмов распознавания с учетом возможности спуфинга. Существенно более стойкой к спуфингу является новая 3D-технология 3D Hybrid Face Recognition, которая учитывает не только текстуру человеческого лица, но и его форму [3].

В докладе рассматриваются общие методы противодействия атакам спуфинга в биометрических системах, а также методы и средства обнаружения спуфинг-атак с использованием алгоритмов выявления принадлежности вводимых для идентификации изображений лиц живым или неживым объектам.

Особое внимание уделяется алгоритмам, основанным на анализе движения глаз в последовательности изображений и слежения за лицами в реальном времени. Применение таких алгоритмов при идентификации позволяет существенно повысить стойкость разрабатываемых систем к спуфингу.

Литература

1. Biometrics Market and Industry Report 2009–2014 [Электронный ресурс]. Режим доступа: http://www.biometricgroup.com/reports/public/market_report.php.
2. Технология защиты данных Face Recognition пока еще очень ненадежна [Электронный ресурс]. Режим доступа: http://itnews.com.ua/45334.html.
3. Новая технология идентификации человека по лицу [Электронный ресурс]. Режим доступа: http://itnews.com.ua/41940.html.