

ЭЛЕКТРОННЫЙ ЗАМОК С ДАТЧИКОМ ОТПЕЧАТКА ПАЛЬЦЕВ «TOUCH LOCK»

А.Д. Курилова, Д.Е. Новицкий, И.И. Савенко
Томский политехнический университет
3208607970@mail.ru

Введение

Замок является важной составляющей двери. От его надежности и качества будет зависеть безопасность вашего имущества.

Всем давно известны достоинства и недостатки традиционных механических дверных замков. Достоинств много, а главных недостатков два:

1 Все существующие на сегодняшний день механические замки выпускаются уже не менее 15-и лет, поэтому их конструкция и методы вскрытия не являются секретом для “заинтересованных лиц”.

2 Так как ключевые отверстия таких замков видны с внешней стороны, то определить марку, тип и расположение дверного замка не составляет труда.

Поэтому устанавливать электронные замки намного надежней. Электронные замки делятся на несколько типов:

1 Замки с системой аутентификации сетчатки глаза. Преимущества: алгоритм статически надежен. Недостатки: высокая цена и низкая доступность готовых решений.

2 Кодовый замок. Опять же не нужно использовать ключи, но код можно забыть или его могут подсмотреть при вводе.

3 Замки с RFID-меткой. Преимущества: удобство в использовании, возможность замаскировать считыватель метки так, что визуально замок не будет виден, что повышает защищенность от взлома. Недостатки: RFID-метку возможно скопировать легко и незаметно для владельца.

4 Замок с датчиком отпечатка пальца.

Технологии устройства «Touch Lock»

Биометрические замки начали развиваться в 90-х годах XX века вместе со скачком развития биометрических технологий, когда сенсоры, распознающие папиллярный узор пальца, стали намного точнее. Такие замки еще называют дактилоскопическими или смартлоками.

Помимо способности распознавания по отпечаткам, биометрические замки имеют все характеристики и функции обычных механических замков. Также по надежности, секретности и взломостойкости биометрические замки на сегодняшний день стали превосходить механические устройства среднего и высокого класса. Помимо этого, они избавляют от ключей, магнитных карт, запоминания кодовых комбинаций. Так что вероятность остаться за закрытой дверью, потому что потерял

ключ или забыл код, невелика [1].

Наиболее проработанный на сегодняшний день биометрический метод идентификации личности – это распознавание отпечатка. У каждого человека свой уникальный папиллярный узор на пальцах, благодаря этому и возможна идентификация. Классические алгоритмы используют характерные точки в узоре: конец, разветвление линии узора, одиночные точки. К тому же используется информация о морфологической структуре папиллярного узора: положение замкнутых, спиральных и “арочных” линий друг относительно друга. Уникальные характеристики отпечатка преобразуются в код, сохраняющий информацию об изображении отпечатка, этот код и хранится в базе данных, которая используется для хранения и сравнения отпечатков. Время транслирования изображения папиллярного узора в код и идентификации чаще всего не превышает одной секунды, но имеет зависимость от размера базы данных. Время, затрачиваемое на поднесение руки, не учитывается.

Одним из таких биометрических замков является «Touch Lock». Интегрированный в модуль датчик отпечатков пальцев выполняет ряд функций, таких как регистрация отпечатков, обработка изображений, идентификация, поиск и хранение шаблонов.

«Touch Lock» довольно прост в эксплуатации: палец прикладывается к сенсору, считывается его отпечаток, и если находится соответствие в базе данных, тогда замок открывается [2].

Принцип обработки отпечатка пальца

Устоявшимися понятиями для биометрии являются — False Acceptance Rate (*FAR*) и False Rejection Rate (*FRR*). Первое понятие характеризует шанс ложного совпадения биометрических характеристик двух разных людей. Второе же – вероятность запрета доступа человеку, который имеет допуск. Система биометрии тем качественнее, чем меньше у неё *FRR* при том же *FAR*.

Для понимания значения вероятностей *FAR* и *FRR*, можно оценить, насколько часто будут проявляться ложные совпадения, если система идентификации будет установлена в организации размером в *N* человек. Шанс неверного совпадения отпечатка пальца полученного сканером для базы данных из *N* отпечатков равен $FAR * N$. Порядка *N* человек проходит через пункт контроля доступа каждый день. В таком случае вероятность ошибки в течение рабочего дня будет равна $FAR * (N^2)$. Если допустима одна ошибка в течение рабочего

дня, тогда: $FAR * N^2 \approx 1 \Rightarrow N \approx \sqrt{\frac{1}{FAR}}$

Стандартное значение FAR для датчиков отпечатка пальца – 0.001%.

Соответственно из формулы получаем, что система идентификации при $FAR=0.001\%$ будет стабильно работать с численностью персонала $N \approx 300$.

Преимуществами данного метода являются: высокая достоверность — статистические показатели метода выше, чем у методов идентификации по лицу, голосу, росписи; невысокая цена устройств, предназначенных для сканирования отпечатка пальца; несложная процедура сканирования отпечатка.

Недостатком является легкое повреждение папиллярного узора отпечатка пальца мелкими порезами, царапинами. Люди, которые использовали сканеры отпечатка пальца в фирмах числом порядка сотен человек, говорят об относительно высокой частоте отказа сканирования. Ещё на текущем уровне технологий есть возможность относительно просто подделать изображение отпечатка [3].

Используемым сканером отпечатков пальцев в проекте «Touch Lock» является «ZFM-20» от компании Adafruit. В качестве системы управления используется Arduino Mega2560, программирование которой происходит на языке «Wiring». База данных с соответствиями отпечатков людям на текущий момент хранится в EEPROM (постоянной энергонезависимой памяти) Arduino.

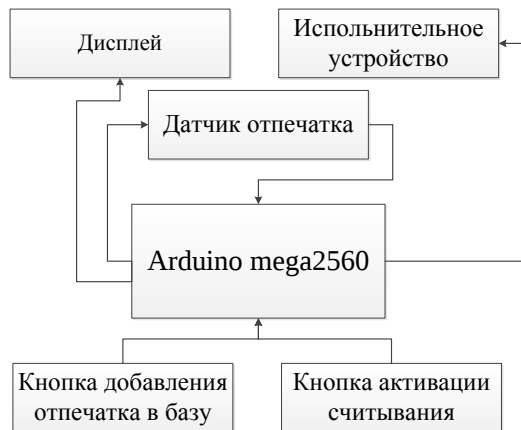


Рис. 1. Схематическое устройство «Touch Lock»

Перспективы

В дальнейшем планируется два варианта развития: в первом управляющая программа и база данных находятся на сервере, а Arduino используется лишь как исполняющее устройство команд сервера, во втором база данных будет храниться на съёмном носителе, подключаемом напрямую к Arduino, а обработка будет вестись ею самой. Так же планируется замена Arduino на обычный мик-

роконтроллер AVR серии ATmega, для удешевления и упрощения устройства. Ещё будут добавлены часы реального времени, позволяющие контролировать время прихода и ухода сотрудников (при установке на предприятии), так же это нововведение позволит задавать индивидуальное время доступа для каждого человека, т.е. кто-то может заходить всегда, а кто-то, например уборщики, лишь в стандартное время уборки. Помимо этого в устройство будет добавлен датчик температуры и влажности, что позволит легко контролировать эти параметры в комнате. Планируется добавление графического дисплея с удобным выводом меню для управления всеми функциями замка.

На текущий момент «Touch Lock» питается от сети переменного тока через блок питания, на случай отключения сети электроснабжения будет добавлено резервное питание от аккумулятора и схема для его зарядки. Ещё, возможно, будет добавлен внешний разъем для подключения батареи «Крона», чтобы гарантировать возможность открытия двери даже при очень длительном отключении электроэнергии.



Рис. 2. Отпечаток пальца

Литература

- 1 Интернет версия журнала «Barlette» [Электронный ресурс]. - Режим доступа: <http://barlette.ru/journal/article/505.html>, свободный
- 2 Сайт электронного биометрического замка «Touch Lock» [Электронный ресурс]. - Режим доступа: <http://projecteee.devyourself.ru/co/TouchLock/>, свободный
- 3 IT-сообщество «Хабрахабр» [Электронный ресурс]. - Режим доступа: <http://habrahabr.ru/post/126144/>, свободный