отнести тот факт, что все действия с по работе с веб-страницей объединены в одном месте. При использовании данного паттерна, все описания элементов, а также методы взаимодействия с этими элементами описываются в PageObject классе тестируемой страницы. Методы взаимодействия, в свою очередь, вызываются из классов-тестов, описывающее порядок выполнения действий по взаимодействию с веб-страницей.

Плюсы автоматизации тестирования очевидны: быстрое выполнение, исключение «человеческого фактора», возможность высвобождения времени тестировщика, а также автоматическая генерация отчётов. Но существует и ряд минусов, основным из которых можно назвать трудоёмкость – несмотря на то, что автоматические тесты позволяют устранить ручное выполнение части однотипных операций и непосредственное выполнение тестирования, много затрат может приходиться на поддержку в актуальном состоянии самих тестов после изменения функциональности приложения.

Второй недостаток автоматизации – однотипность: все автоматизированные тесты выполняются строго по заложенному сценарию. При прохождении теста вручную сотрудник команды тестирования может обратить внимание на другие детали в приложении, изменить логику выполнения теста и обнаружить дефект, который был бы проигнорирован автоматическим тестом.

Следует помнить, что процесс автоматизации тестирования – это дополнение к тестированию, повышающее его эффективность за счёт уменьшения затрат. При постановке задачи внедрения автоматизированного тестирования в процесс создания образовательных ресурсов стоит учитывать возможность появления дополнительных затрат времени и иных ресурсов. Поэтому одной из важных задач подразделения тестирования является выбор степени автоматизации процесса тестирования программного продукта, в том числе и образовательного ресурса.

Таким образом, для веб-приложений, будь это электронные библиотеки, интернет-магазины или системы автоматизации производства, очень важна корректность работы, способность выдерживать большие нагрузки, соответствие заданным требованиям безопасности и т.д. Автоматизированное тестирование может значительно ускорить проведение тестов, которые позволяют удостовериться в том, что функциональность предыдущих версий всё корректно работает в текущей сборке приложения, а само приложение корректно работает на различных конфигурациях и окружениях. Так же автоматические тесты могут проводить проверки работы атомарных участков кода и взаимодействий между модулями приложения. Например, для систем управления предприятием, где несанкционированный доступ в систему недопустим, авто-тесты могут проводить различные проверки безопасности: прав доступа, открытых портов, уязвимостей в текущих версиях ПО и т.д. А автоматический тест, направленный на то, чтобы удостоверится что производительность приложения не падает при больших объемах данных, например, в базе данных, будет актуален для интернет-магазинов.

Список использованных источников:

1. Гленфорд Майерс, Том Баджетт, Кори Сандлер. Искусство тестирования программ, 3-е издание (TheArtofSoftwareTesting, 3rdEdition.) — М.: «Диалектика», 2012. — 272 с.
2. Святослав Куликов. Тестирование программного обеспечения. Базовый курс. — EPAM Systems, 2015-2016, 288 с.
3. Про Тестинг [Электронный ресурс] // protesting.ru : Тестирование Программного Обеспечения. URL: http://www.protesting.ru/automation (дата обращения: 15.01.2017).

АУТЕНТИФИКАЦИЯ ПО РАДУЖНОЙ ОБОЛОЧКЕ ГЛАЗА

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Чечет А.С.

Прохорчик Р.В. - м.т.н., ассистент

Существует несколько способов контроля предоставления доступа к информации. Одним из них является аутентификация. Аутентификация – это процесс, в ходе которого на основании пароля, ключа или какой-либо иной информации, пользователь подтверждает, что является именно тем, за кого себя выдает.

Для более подробного рассмотрения была выбрана аутентификация по биометрическим признакам, а именно по радужной оболочке. Это достаточно перспективное направление, поскольку для ее реализации необходима лишь обычная камера. Несколько лет назад фотоаппараты обладали камерами в 1-3Мп а сегодня мы можем позволить себе телефон с 20Мп. С течением времени качество камер будет усиливаться, что может позволить получать качественное изображении глаза даже на мобильном телефоне. Уже существуют телефоны с возможностью аутентификации по отпечатку пальца, например Apple iPhone 6 128Gb, Honor 7, Samsung Galaxy S7.

Рисунок 1 Область распознавания

Рисунок 2 Преобразованная в прямоугольник радужная оболочка

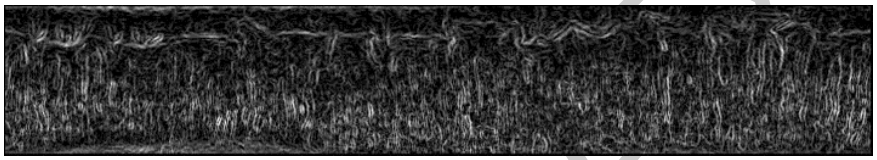

Рисунок 3 Градиент радужной оболочки

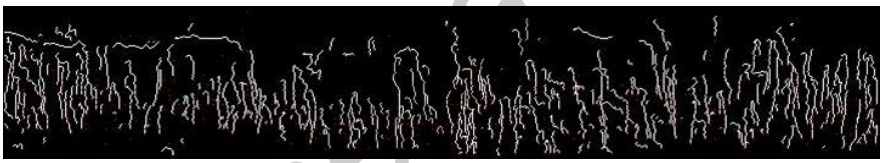

Рисунок 4 Выделенные по градиенту ключевые линии

Для аутентификации по радужной оболочке необходимо получить изображение глаза. Далее следует выделить окружность радужной оболочки и зрачка (рисунок 1). Полученное пространство между двумя окружностями для удобства работы рекомендуется преобразовать в прямоугольное изображение используя полярную систему координат для перевода (рисунок 2). Одним из вариантов дальнейшей обработки может быть такая последовательность действий:

- Формирование черно-белого изображения;
- Получение градиента изображения (рисунок 3);
- Детектирование ключевых линий (рисунок 4);
- Нахождение расстояния Хэминнга между проверяемым изображением и хранимым эталоном
- Проверка значения расстояния с возможно допустимым;
- Получение доступа или отказ.

Естественно современные системы позволяют хранить десятки тысяч изображений в базе, однако успевать обрабатывать их в реальном времени способны далеко не все системы. Поэтому следует минимизировать объем информации для хранения в базе, так как он будет сверяться в режиме реального времени с полученным изображением.

У сканера радужной оболочки есть свои достоинства и недостатки. К недостаткам можно отнести возможность взлома через обычное качественное изображение глаза. К достоинствам можно отнести отсутствие дорогостоящего дополнительного оборудования, достаточно лишь хорошей встроенной камеры телефона, уверен что у многих уже есть фронтальные камеры более 5Мп.

Все хотят получать доступ к скрытой информации максимально легко, при этом максимально обезапасив ее от проникновения злоумышленника. С развитием средств вычислительнй техники появляются все более сложные и надежные варианты защиты. Алгоритмы аутентификация и качество оборудования улучшаются с каждым днем и мы можем начать использовать более надежные способы биометрической аутентификации, к примеру по радужной оболочке. И с скором времени для доступа не будет необходимости запоминать сложные пароли, а надо будет лишь посмотреть в камеру.

Список использованных источников:

1. Википедия Свободная энциклопедия [Электронный ресурс] – Режим доступа : https://ru.wikipedia.org/wiki/Аутентификация_по_радужной_оболочке_глаза. Дата доступа: 01.04.2017.