происходит анализ биометрических характеристик и тут же корректировка эталона.

Недостаток такой системы анализа клавиатурного почерка заключается в том, что если пользователь находится в возбужденном состоянии, под воздействием психотропных препаратов, алкогольного опьянения или просто болен, то стабильность параметров работы нарушается, и процесс сквозной аутентификации может стать серьезной проблемой.

Таким образом, для повышения достоверности аутентификации пользователя не только при входе в систему, а так же в процессе работы, необходимо использовать комбинированный метод, сочетающий в себе стандартные процедуры ввода паролей на начальном этапе и анализа характерного поведения зарегистрированного пользователя на всём протяжении работы в защищённой системе.

И.Н. Ефимов, А.М. Косолапов

КЛАССИФИКАЦИЯ СПОСОБОВ ПОДТВЕРЖДЕНИЯ ПОДЛИННОСТИ РАСПОЗНАВАЕМОГО ОБЪЕКТА[2]

(Самарский государственный университет путей сообщения)

Системы автоматического распознавания лиц находят все большее применение в биометрических системах безопасности, контроля и управления доступом пользователей. Однако нельзя доверять системам, не использующим защиту от спуфинг (spoofing) атак. Для биометрических систем спуфинг — это обман путём предоставления биометрическому сенсору копий, муляжей, фотографий, видеозаписи, заранее записанных звуков и т. п. Цель атаки спуфинга при распознавании — представление незарегистрированного пользователя в системе как зарегистрированного. В [9] авторы продемонстрировали, успешный взлом коммерческих систем распознавания лиц, используя фотографию или видеозапись зарегистрированного пользователя с экрана устройства. Защита от спуфинг атак является трудоёмкой задачей, так как злоумышленник имеет непосредственный контакт с видеокамерой, поэтому невозможно использовать различные криптографические методы защиты. Наилучшие результаты, по данным разработчиков, продемонстрировали системы использующие специализированные сканеры или видеокамеры, позволяющие реконструировать 3D объект. Тем не менее, способы подтверждения подлинности объекта, не использующие специализированное оборудование и не требующие дополнительных действий, наиболее перспективны, т.к. удобнее для конечного пользователя и могут быть легко интегрированы в существующие системы распознавания лиц.

[2] Работа поддержана грантом фонда содействия развитию малых форм предприятий («У.М.Н.И.К.» I полугодие, Самара, 2014).

В работе предложена новая классификация известных способов подтверждения подлинности распознаваемого объекта в зависимости от реализации. Существующие классификации не отражают все многообразие известных способов подтверждения подлинности распознаваемого объекта (СППРО) и нуждаются в пересмотре и дополнении. СППРО разделяются в зависимости от вида воздействия на распознаваемый объект: способы с физическим воздействием (СФВ), с командным (СКВ) и без воздействия (СБВ). Оригинальная классификация СППРО представлена на рисунке 1.

Для функционирования способов, основанных на командном воздействии, пользователю необходимо произвести некоторые действия в указанный системой защиты момент: произнести сгенерированный случайный текст, моргнуть или открыть рот, продемонстрировать различные эмоции и т.д. Способы с физическим воздействием можно условно разделить на:

- способы, применяющие ИК излучение (ИКИ), с последующим анализом следующих характеристик: оптических свойств (ОС) человеческой кожи и зрачков, рельефной структуры (РС) объекта и т.д.;
- способы, применяющие видимый спектр света (ВСС), с последующим анализом следующих характеристик: оптических свойств (ОС) человеческой кожи, реакции зрачков (РЗ), рельефной структуры (РС) объекта и т.д.

Способы без воздействия на объект разделяют на:

- способы, анализирующие текстурные признаки (АТП): локальные бинарные шаблоны (ЛБШ), гистограммы ориентированных градиентов и т.д.;
- способы, использующие построение 3D модели объекта с помощью: карт глубин, аффинного преобразования, сканера или видеокамер и т.д.;
- способы, использующие обнаруженные биофизические признаки (ОБП): движение глаз, моргание, мимика, движение головы относительно фона, кровеносные сосуды, термограмма и т.д.

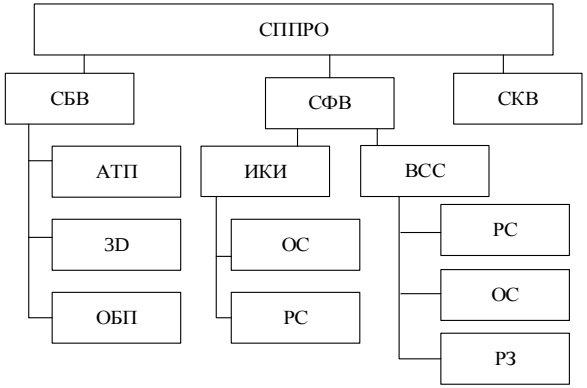

Рисунок 1 – Классификация СППРО

Ниже представлены различные примеры СППРО, не использующие воздействие на распознаваемый объект. Существует целый ряд работ, в которых

для обнаружения подмены используются различные текстурные признаки: ЛБШ и метод опорных векторов (вероятность верного признания объекта не менее 91,2% и вероятность пропуска злоумышленника не более 0,2%) [8], ЛБШ и искусственные нейронные сети (вероятность правильного распознавания составила 97,5% на базе двумерных изображений) [13], вейвлеты Габора [11], гистограммы ориентированных градиентов [15], пространственно-временные дескрипторы [7] и т.д. В работе [8] приведены результаты экспериментальных исследований различных СППРО, которые используют текстурные признаки. Вероятность ошибки в среднем достигла 15%, когда СППРО сталкивались с широким набором типов спуфинг атак в экспериментальной базе данных. Другая категория методов сосредоточилась на обнаружении биофизических признаков распознаваемого объекта. В [6] представлен ряд методов основанных на: скорости моргания, анализе движения глаз, рта или головы относительно фона. Методы используют поле оптического потока для оценки движения. Ошибка распознавания для данных методов составила не более 8,98%. Следующие СППРО основаны на анализе термограммы или рисунка поверхностных кровеносных сосудов распознаваемого объекта [5]. Преимущество применения подобных алгоритмов перед стандартными заключается в их относительной нечувствительны к изменению освещения. Подтверждение подлинности основано на том, что реальные, в отличие от искусственных, объекты излучают различный диапазон инфракрасного излучения или имеют поверхностные кровеносные сосуды. В работе [10] выполняется восстановление 3D-модели лица с помощью аффинного преобразования, без необходимости вмешательства пользователя и дополнительных аппаратных средств.

Для функционирования представленных ниже СППРО требуется физическое воздействие на распознаваемый объект. В работе [1] представлен подход к обнаружению подмены на основе анализа спектральных характеристик отражения кожи лица человека. Представлен алгоритм защиты от спуфинг атак, в ходе которого с помощью сенсора формируют изображения распознаваемого объекта при различных длинах волн и анализируют спектральные характеристики поверхности объекта. Авторы работы говорят о следующих результатах FAR = 0,05, FRR = 0,09 на тестовой выборке, включающей изображения двадцати реальных человек, трёх силиконовых масок и трёх фотографий лица. В работе [2] для подтверждения подлинности распознаваемого объекта используются изображения зрачков пользователя. В данном изобретении защита от спуфинга основана на свойстве человеческого зрачка – сужаться при повышении интенсивности света. Чтобы узнать получено изображения пользователя с глаза живого человека, а не с его муляжа, варьируют интенсивность освещения. Система регистрации изображений отслеживает реакцию зрачка на модуляцию, для чего время регистрации немного увеличивают. В [12] подтверждение подлинности основано на свойстве человеческого зрачка – отражать падающее на него изображение. Представлен алгоритм, в ходе которого, изображения проецируются на экране компьютера. Изображения отразятся от зрачка пользователя и будут захвачены видеокамерой.

Для функционирования представленных ниже СППРО требуется командное воздействие на распознаваемый объект. В работе [14] для подтверждения подлинности распознаваемого объекта используются изображения, полученные в обычном состоянии и в состоянии, когда пользователю требуется выполнить предложенное системой действие. Набор действий не повторяется, действия могут быть следующими: открыть или закрыть глаза, закрыть один глаз, закрыть или открыть рот и т.д. В [4] описан метод и реализация системы распознавания пользователей с использованием лица, голоса и жестов. На первом этапе выполняется анализ изображения лица человека, захваченного видеокамерой. Полученные данные сравниваются с шаблонами из базы данных, и принимается решение о предоставлении доступа. Дальнейшее взаимодействие с системой осуществляется при помощи голоса и жестов. Система производит сравнение каждой подаваемой команды с шаблонами из базы данных и предоставляет доступ к запрашиваемой операции только при положительном результате проведённого сравнения. В работе [3] пользователю необходимо смотреть в чётко указанные на мониторе места, выставленные случайным образом, после чего программа анализирует траекторию движения глаз пользователя. Разработчики метода пишут о 95% вероятности верного распознавания подмены, на БД, содержащей двумерные изображения распознаваемого объекта.

Приведённая классификация позволяет выявить дальнейшие пути развития СППРО и позволяет ориентироваться в многообразии существующих технических решений.

Литература

1. Костылев Н.М. Модуль обнаружения витальности лица по спектральным характеристикам отражения кожи человека / Н. М. Костылев, А. В. Горевой // Инженерный журнал наука и инновации – 2013. – Т. 9 – 1–13с.

2. Способ И.Л. Способ идентификации личности по радужной оболочке глаза (варианты) : пат. 2407435 C1 Рос. Федерация / И. Л. Способ – 2009.

3. Adamiak K. Liveness detection in remote biometrics based on gaze direction estimation / K. Adamiak, D. Zurek, K. Slot // Proc. Fed. Conf. Comput. Sci. Inf. Syst. – 2015. – Т. 5 – 225–230с.

4. Automatic access to Automatic access to an automobile via biometrics : пат. 6498970 США / access to Automatic – 2002.

5. Bhowmik M.K. Thermal Infrared Face Recognition-A Biometric Identification Technique for Robust Security System / M. K. Bhowmik, A. N. Sarma, A. Saha, D. Bhattacharjee, D. K. Basu, G. Majumder, K. Saha, M. Nasipuri, S. Majumder // Rev. Refinements New Ideas Face Recognit. – 2011. – Т. 6 – 113–139с.

6. Chakraborty S. An overview of face liveness detection / S. Chakraborty, D. Das // Int. J. Inf. Theory – 2014. – Т. 13 – № 2 – 11–25с.

7. Chingovska I. On the Use of Client Identity Information for Face Antispoofing / I. Chingovska, A. dos Anjos // Inf. Forensics Secur. IEEE Trans. – 2015. – Т. 10 – № 4 – 787–796с.

8. Chingovska I. On the Effectiveness of Local Binary Patterns in Face Antispoofing , 2012.

9. Duc N.M. Your face is not your password , 2009. – 16c.

10. Liveness detection method Liveness detection method and apparatus of video image : пат. 8355530 США / detection method Liveness – 2013.

11. Maatta J. Face spoofing detection from single images using micro-texture analysis , 2011.

12. Methods for performing Methods for performing biometric recognition of a human eye and corroboration of same : пат. 8260008 США // – 2012.

13. REKHA P.S. Spoofing Face Recognition Using Neural Network with 3D Mask / P. S. REKHA // Int. J. Emerg. Technol. Comput. Sci. Electron. – 2015. – Т. 14 – № 1 – 123–127c.

14. Secure biometric authentication Secure biometric authentication from an insecure device: заяв. пат. 12/960,511 США / biometric authentication Secure – 2010.

15. Yang J. Face liveness detection with component dependent descriptor , 2013. – 1–6c.

В.А. Заступов, М.В. Кузнецов

ЦИКЛИЧЕСКАЯ АУТЕНТИФИКАЦИЯ НА ОСНОВЕ ТРАДИЦИОННЫХ ДЕЙСТВИЙ ПОЛЬЗОВАТЕЛЯ

(Поволжский государственный университет
телекоммуникаций и информатики)

Мы живем в информационном веке. Ежедневно взаимодействуем с электронными устройствами, храним свои данные на информационных носителях и в памяти компьютера, используем интернет ресурсы для работы и проведения досуга. В наше время, вопрос о защите информации является одним из основных практически в любой сфере деятельности.

На данный момент существует множество методов защиты системы от несанкционированного доступа. Из них можно выделить стандартные (ввод логина/пароля, ответ на секретный вопрос, ввод пин-кода) и более сложные системы защиты, построенные на использовании уникального предмета (электронный ключ, магнитная карта и т.д.).

Данные методы имеют недостатки, главным из которых является то, что в случае, когда злоумышленнику удается заполучить необходимую информацию для проникновения в систему (будь то пароль или материальный атрибут) происходит имитация санкционированного доступа и все ресурсы автоматически становятся доступны для использования. Именно решение этой проблемы и стоит в основе данной работы.

Все мы слышали фразу о том, что каждый человек уникален. На этом факте были созданы биометрические системы защиты такие как: сканирование сетчатки глаза, отпечатков пальцев, формы лица и т.д. Все эти системы представляют собой дорогостоящие устройства и в большинстве своем имеют одношаговый этап аутентификации. Циклическая аутентификация на основе традиционных действий пользователя – это метод, не прекращающий действие на протяжении всего взаимодействия пользователя с персональным компьютером, прост и дёшев в реализации, имеет возможность работать в скрытном режиме (незаметно для пользователя). Также важной особенностью является то, что данная идея позволяет аутентифицировать пользователя при работе с интернет ресурсами.

Принцип работы циклической аутентификации состоит из трёх этапов:

1) Этап обучения. При работе с персональным компьютером мы часто сталкиваемся с действиями, которые можно выполнить различными способами (переключение языка, работа с буфером обмена, сохранение документа и т.д.). Каждый пользователь выполняет все эти действия, исходя из своих привычек, выработанных за время работы с ПК. Задачей этапа обучения является фиксация таких действий и способов их выполнения. Данный этап выполняется при помощи программного обеспечения «Кейлогер», позволяющее осуществлять контроль над деятельностью пользователя персонального компьютера, фиксировать действия мышью, набор горячих клавиш. По истечению времени обучения, формируется лог-файл.

2) Этап формирования портрета пользователя. Имеющийся лог-файл зашифровывается и отправляется на удаленный сервер безопасности. По прибытии файл расшифровывается, производится анализ данных, нахождение закономерностей, выявление особенностей и, в итоге, формирование индивидуального портрета пользователя - эталон. Необходимо отметить, что после продолжительного времени работы с такой системой необходимо вносить изменения в эталонные характеристики, поскольку «привычки» со временем имеют свойство меняться.

3) Этап аутентификации. На данном этапе происходит непосредственно сравнение действий пользователя с эталоном в реальном времени при работе за ПК. В случае, когда процент несоответствий превышает заданный порог доверия, система автоматически отключается и на сервер безопасности отправляется сигнал о несанкционированном доступе.

Для доказательства эффективности данного метода было произведено анкетирование среди постоянных пользователей ПК. Опрашиваемому предлагался список действий и методы его выполнения, из которых он должен был выбрать тот, каким наиболее часто пользуется.

Всего было предоставлено 44 действия и на каждое действие минимум 4 варианта ответа. Также был отдельно произведен опрос касательно сочетания правого и левого Shift-ов с той или иной клавишей на клавиатуре. Участие приняло свыше 80-ти человек.

Проанализировав полученные результаты, было установлено, что самое ближайшее совпадение между традиционными действиями двух пользователей составило 80%, среднее число совпадений составило 46%, минимальное совпадение между двумя пользователями составило 16%. С учетом максимального совпадения в 80% мы имеем 20-ти процентное несоответствие индивидуальных