НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ
май–июнь 2018 Том 18 № 3 ISSN 2226-1494 http://ntv.ifmo.ru/
SCIENTIFIC AND TECHNICAL JOURNAL OF INFORMATION TECHNOLOGIES, MECHANICS AND OPTICS
May–June 2018 Vol. 18 No 3 ISSN 2226-1494 http://ntv.ifmo.ru/en

УДК 004.4

ИСПОЛЬЗОВАНИЕ СИСТЕМЫ РАСПОЗНАВАНИЯ ЛИЦ ДЛЯ ОСУЩЕСТВЛЕНИЯ ПОКУПОК В МОБИЛЬНЫХ УСТРОЙСТВАХ И ВЕБ-ПРИЛОЖЕНИЯХ

Д.В. Иванько[a]

[a] Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация
Адрес для переписки: dmitriy_ivanko@yahoo.com

Информация о статье
Поступила в редакцию 09.02.18, принята к печати 16.03.18
doi: 10.17586/2226-1494-2018-18-3-457-461
Язык статьи – русский

Ссылка для цитирования: Иванько Д.В. Использование системы распознавания лиц для осуществления покупок в мобильных устройствах и веб-приложениях // Научно-технический вестник информационных технологий, механики и оптики. 2018. Т. 18. № 3. С. 457–461. doi: 10.17586/2226-1494-2018-18-3-457-461

Аннотация
Рассмотрена проблема установления личности клиента при проведении платежной операции с использованием мобильных устройств и веб-приложений. Обозначены стандартные способы идентификации пользователей при проведении платежной операции. Обсуждены основные критерии качества систем идентификации в мобильных устройствах и веб-приложениях, такие как точность правильного распознавания современных клиент-серверных систем, среднее время идентификации, возможность распределения вычислений, а также удобство использования. Особое внимание уделено вычислительным и временным затратам, поскольку они являются наиболее существенными для клиентов, использующих практически применимые мобильные и веб-приложения. Обозначены преимущества и недостатки применения систем распознавания лиц для проведения идентификации. Дано описание каждого элемента системы, участвующего в проведении безопасной банковской транзакции в процессе осуществления платежной операции. Представлена клиент-серверная модель взаимодействия системы распознавания лиц для обеспечения безопасности при совершении покупок с использованием мобильных устройств или веб-приложений. Приведены экспериментальные оценки среднего времени идентификации для систем распознавания лиц. Разработанная модель взаимодействия позволила сократить затрачиваемое клиентом на транзакцию время в среднем на 47% по сравнению с использованием стандартных средств идентификации.

Ключевые слова
системы распознавания лиц, платежные системы, клиент-серверные приложения, веб-приложения, мобильные устройства и мобильные приложения

Благодарности
Работа выполнена при поддержке Министерства образования и науки Российской Федерации, госзадание № 8.9957.2017/5.2.

FACE RECOGNITION SYSTEM FOR PAYMENT PROCESS ON MOBILE DEVICES AND WEB-APPLICATIONS

D.V. Ivanko[a]

[a] ITMO University, Saint Petersburg, 197101, Russian Federation
Corresponding author: dmitriy_ivanko@yahoo.com

Article info
Received 09.02.18, accepted 16.03.18
doi: 10.17586/2226-1494-2018-18-3-457-461
Article in Russian

For citation: Ivanko D.V. Face recognition system for payment process on mobile devices and web-applications. *Scientific and Technical Journal of Information Technologies, Mechanics and Optics*, 2018, vol. 18, no. 3, pp. 457–461 (in Russian). doi: 10.17586/2226-1494-2018-18-3-457-461

Abstract
The paper deals with the problem of users' identity authentication during payment transactions with the use of mobile devices and web applications. Standard methods of users' identification are considered at performing a payment transaction. The subjects of discussion are the main criteria for the effectiveness of user identification systems in mobile devices and web applications, such as the identification accuracy of the modern systems, time and computational costs, the ability to distribute computations and user convenience. Particular attention is paid to computational and time costs, as they are the most

significant for users who make use of practically applicable client-server mobile and web applications. The advantages and disadvantages of face recognition systems application for users' identification and verification are pointed out. Each system element participating in secure banking transaction is described in the course of the payment transaction. A new client-server model is presented for interaction of the face recognition system for security assurance while shopping with the use of mobile devices or web applications. Experimental estimates of the face recognition systems effectiveness are also given. The developed architecture gave the possibility to reduce the time spent by the client for the transaction by an average of 47%, compared with application of standard user authentication tools.

Keywords
face recognition systems, payment systems, client-server applications, web-applications, mobile devices and software

Acknowledgements
This paper was supported by the Ministry of Education and Science of the Russian Federation, state project No. 8.9957.2017 / 5.2.

Введение

Биометрические системы распознавания лиц достигли значительного прогресса в последние несколько десятков лет. В определенных условиях точность правильного распознавания таких систем превосходит человеческий уровень [1, 2]. Автоматическое распознавание лиц все больше применяется в повседневной жизни людей [3–5], охране общественного порядка [6] и контроле управления доступом [7].

Биометрическая технология распознавания лиц (Face Recognition Technology) охватывает методы и средства, предназначенные для решения задач аутентификации и идентификации человека на основе изображения лица ([8], стр. 12). В настоящей работе будет рассматриваться только задача идентификации человека. Под идентификацией понимается сравнение предъявляемого идентификатора (изображения лица) с перечнем присвоенных идентификаторов.

В данной работе, в соответствии с определениями ГОСТ[1,2], объектом доступа является информация для осуществления платежа, хранимая на стороннем сервере. Субъектом доступа является пользователь мобильного и (или) веб-приложения, осуществляющий доступ к объекту. В работе предлагается использование изображения лица в качестве идентификатора для осуществления доступа.

Современные платежные системы предлагают весьма сложную систему безопасности, распределенную между клиентом, сервером приложения и сервером платежной системы. К тому же все больше идентификаторов требуется от пользователя для совершения покупки: номер карты, дата окончания действия, контрольный номер, код с SMS-подтверждением и другая информация. При этом вся вводимая информация служит одной единственной цели – идентификации пользователя, совершающего покупку. Системы распознавания лиц позволяют естественным образом идентифицировать человека, совершающего покупку. Большинство современных мобильных устройств оснащены цифровыми камерами. Основным преимуществом систем распознавания лиц является время, необходимое пользователю для проведения покупки. Эксперименты, проводимые в работе, показали уменьшение затрачиваемого времени на 47% по сравнению с использованием стандартных средств идентификации. Помимо этого, пользователю после однократной регистрации на сервере системы распознавания лиц нет необходимости постоянно иметь при себе большое количество перечисленных выше идентификаторов, что также увеличивает удобство использования таких систем.

В первой части настоящей работы представлена предлагаемая клиент-серверная модель взаимодействия системы распознавания лиц для обеспечения безопасности банковских транзакций. Во второй части представлена оценка точности правильного распознавания и среднего времени идентификации.

Взаимодействие системы распознавания лиц и платежных систем

Проведение платежных транзакций осуществляется по схеме, представленной на рисунке.

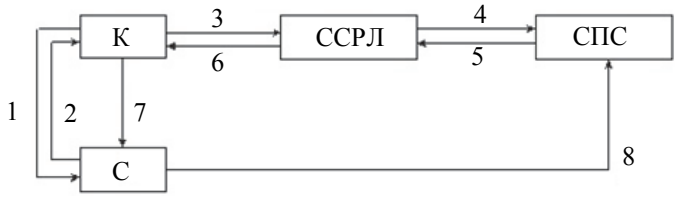

Рисунок. Клиент-серверная модель взаимодействия системы распознавания лиц, платежных систем и сторонних приложений

[1] ГОСТ Р 52633.0-2006. Национальный стандарт защиты Российской Федерации. Защита информации. Техника защиты информации. Требования к средствам высоконадежной биометрической аутентификации. Введ. 01.01.10. М.: Изд-во стандартов, 2010. 20 с.

[2] Защита от несанкционированного доступа к информации. Термины и определения [Электронный ресурс]. Режим доступа: https://fstec.ru/component/attachments/download/298, свободный. Яз. рус. (дата обращения 20.03.2018).

Основными элементами взаимодействия являются:

К – клиентская сторона, которая может быть представлена как мобильным устройством, так и веб-приложением;

С – серверная сторона, сервер приложения, для которого осуществляется покупка и который предоставит ресурс и (или) услугу в случае успешного проведения банковской транзакции;

ССРЛ – сервер системы распознавания лиц, осуществляющий идентификацию, особенности реализации СРЛ представлены в работах [8, 9].

СПС – сервер платежной системы, который ответственен за проведение банковских транзакций. В работе в качестве примера представлена платежная система Braintree PayPal Service, которая позволяет осуществлять банковские транзакции, как с помощью стандартных пластиковых банковских карт, так и с помощью электронных платежных систем PayPal и PayPal Credit. Помимо этого, сервис предоставляет доступ к демо-версии системы Braintree Sandbox, которая позволяет осуществлять имитацию проведения покупки для настраивания, тестирования и исследования систем.

Настройка приложения

Платежные системы поставляют специальное программное обеспечение для взаимодействия с СПС. Оно разделено на две части: первое устанавливается на стороне клиента (К), второе – на стороне сервера (С). Платежные системы поставляют средства разработки приложений для клиентской и серверной стороны, поддерживающие большинство известных языков программирования.

Если используются ССРС, то необходимые для проведения транзакции данные хранятся не у пользователя, а непосредственно на сервере СРЛ.

Проведение безопасной банковской транзакции состоит из шагов, последовательность которых представлена на рисунке.

Шаг 1. Клиент запрашивает у сервера ключ для активизации клиентского оборудования (SDK) платежной системы, подтверждая авторизацию клиента.

Шаг 2. Сервер приложения, используя серверное SDK платежной системы, генерирует ключ и возвращает его клиенту.

Шаг 3. Клиент, используя ключ, полученный с сервера, активирует клиентское SDK. Приложение предлагает пользователю сделать фотографию лица. Далее этот снимок отправляется в ССРЛ.

Шаг 4. После идентификации пользователя система распознавания лиц в случае подтверждения личности предоставляет информацию о его платежных данных в СПС. Платежные данные могут быть различны, если у клиента имеется пластиковая карта банка, то ими чаще всего являются номер карты, месяц и год окончания ее действия, а также контрольный номер карты банка (CVV, CVC или др.).

Шаг 5. Сервер платежной системы, в случае подтверждения данных о клиенте генерирует временный ключ для проведения банковской транзакции. Ключ действует ограниченное время, которое зависит от платежной системы, обычно порядка нескольких часов. Далее СПС возвращает этот временно действующий ключ в ССРЛ.

Шаг 6. ССРЛ возвращает ключ клиенту вместе с краткой информацией о платежных данных.

Шаг 7. Клиент может еще раз посмотреть информацию о покупке, способе оплаты и используемых платежных данных. В случае правильности всех используемых данных клиент подтверждает осуществление покупки. Клиентское оборудование отправляет временно действующий ключ на сервер.

Шаг 8. Серверное SDK использует ключ для проведения банковской транзакции и списания средств с карты клиента.

Шаг 9. В случае успеха серверное оборудование заносит информацию о покупке клиента в базу данных и клиенту предоставляется оплаченная им информация и (или) услуга. Проведение покупки считается успешно завершенным.

На каждом из этапов есть теоретическая вероятность прерывания всей цепочки проведения оплаты. В этом случае в обратной последовательности распространяется информация о причине ошибки, в конечном итоге уведомляется как клиент, так и сервер приложения. В этом случае проведение покупки считается завершенным неуспешно.

Оценка точности правильного распознавания и среднего времени идентификации

В работе рассматривается такой показатель качества работы алгоритма распознавания лиц, как точность правильного распознавания [10]:

$$A = \frac{n_{correct}}{n_{total}},$$

где A – точность правильного распознавания; $n_{correct}$ – количество правильно распознанных изображений лиц; n_{total} – общее количество попыток.

Как отмечалось выше, современные алгоритмы распознавания лиц в подконтрольных условиях достигли значительного прогресса. В табл. 1 представлены результаты десяти наиболее успешных алгоритмов распознавания лиц. Сравнения представлены для наиболее репрезентативной в данный момент

базы изображений лиц – Labeled Face in the Wild (LFW) [11]. Результаты сравнения взяты с официального сайта LFW [2]. Информация о каждой системе распознавания лиц и деталях сравнения может быть также найдена на официальном сайте.

№	Название системы распознавания лиц	Средняя точность классификации	Стандартная ошибка
1	Easen Electron	0,9983	0,0006
2	Glasssix	0,9983	0,0018
3	ReadSense	0,9982	0,0007
4	PingAn AI Lab	0,9980	0,0016
5	YouTu Lab, Tencent	0,9980	0,0023
6	VisionLabs V2.0	0,9978	0,0007
7	Faceter.io	0,9978	0,0008
8	Baidu	0,9977	0,0006
9	AuthenMetric	0,9977	0,0009
10	icarevision	0,9977	0,0030
11	**Среднее**	**0,9980**	**нет данных**

Таблица 1. Оценка точности правильного распознавания. Список ссылок и более детальная информация может быть найдена на официальном сайте результатов LFW [2]

Помимо этого, важным показателем является время, необходимое для проведения идентификации пользователя. К тому же при использовании веб-приложений каждая секунда работы и (или) ожидания пользователя очень важна для приложения [12]. От этого напрямую зависит удовлетворенность пользователя, его желание поделиться приложением и вероятность того, что пользователь в следующий раз вновь вернется к этому приложению. Для оценки среднего времени идентификации систем распознавания и осуществления с их помощью идентификации, а затем и покупки, были проведены экспериментальные исследования.

№	Использование системы	Без ССРЛ, с	Вместе с ССРЛ, с
1	Ввод платежных данных	31,9	–
2	Отправка фотографии	–	14,5
3	Обработка запроса ССРЛ	–	< 1,0
4	Отправка данных по сети	< 1,0	< 2,0
5	**Общее время**	**32,9**	**17,5**

Таблица 2. Оценка среднего времени идентификации

Результаты работы систем приведены в табл. 2. В качестве базы данных использовались сведения, полученные от независимых пользователей, каждого из которых просили провести условную оплату двумя способами, на основе разработанной экспериментальной установки с использованием демо-версии платежной системы Braintree Sandbox.

Заключение

Предлагаемая в работе клиент-серверная модель взаимодействия с использованием систем распознавания лиц для обеспечения безопасности при проведении банковских транзакций помогает значительно сократить время, необходимое пользователю для совершения покупки. Дальнейшая работа в данном направлении будет заключаться в исследовании и оптимизации алгоритмов распознавания лиц для предложенной клиент-серверной модели взаимодействия, а также в рассмотрении алгоритмов, наиболее перспективных с точки зрения точности правильного распознавания и практического применения в клиент-серверных приложениях. Помимо этого, одним из важных этапов дальнейшей работы является эффективная интеграция элементов системы распознавания лиц в предлагаемую модель взаимодействия существующих мобильных устройств и веб-приложений.

Литература

1. Gunther M., Costa-Pazo A., Ding C. et al. The 2013 face recognition evaluation in mobile environment // Proc. Int. Conf. on Biometrics. Madrid, Spain, 2013. doi: 10.1109/ICB.2013.6613024
2. Labeled Faces in the Wild: Results [Электронный ресурс]. Режим доступа: http://vis-www.cs.umass.edu/lfw/results.html, свободный. Яз. англ. (дата обращения 20.03.2018).
3. Vazquez-Fernandez E., Gonzalez-Jimenez D. Face recognition for authentication on mobile devices // Image and Vision Computing. 2016. V. 55. P. 31–33. doi:

References

1. Gunther M., Costa-Pazo A., Ding C. et al. The 2013 face recognition evaluation in mobile environment. *Proc. Int. Conf. on Biometrics*. Madrid, Spain, 2013. doi: 10.1109/ICB.2013.6613024
2. *Labeled Faces in the Wild: Results*. Available at: http://vis-www.cs.umass.edu/lfw/results.html (accessed 20.03.2018).
3. Vazquez-Fernandez E., Gonzalez-Jimenez D. Face recognition for authentication on mobile devices. *Image and Vision Computing*, 2016, vol. 55, pp. 31–33. doi:

10.1016/j.imavis.2016.03.018
4. Casti S., Sorrentino F., Spano L.D., Scateni R. Click and share: A face recognition tool for the mobile community // Proc. Int. Conf. on Image Processing (ICIP). 2014. P. 1952–1956. doi: 10.1109/ICIP.2014.7025391
5. Srirama S.N., Paniagua C., Flores H. Social group formation with mobile cloud services // Service Oriented Computing and Applications. 2012. V. 6. N 4. P. 351–362. doi: 10.1007/s11761-012-0111-5
6. Lochner S.A. Saving face: regulating law enforcement's use of mobile facial recognition technology and Iris scans // Arizona Law Review. 2013. V. 55. N 1. P. 201–233.
7. Arrivals Smart Gate [Электронный ресурс]. Режим доступа: http://www.homeaffairs.gov.au/Trav/Ente/Goin/Arrival/Smartgateor-ePassport, свободный. Яз. англ. (дата обращения 20.03.2018).
8. Кухарев Г.А. Каменская Е.И., Матвеев Ю.Н., Щеголева Н.Л. Методы обработки и распознавания изображения лиц в задачах биометрии / под редакцией Хитрова М.В. СПб.: Политехника, 2013. 388 с.
9. Иванько Д.В. Моделирование системы распознавания лиц с использованием мнемонического описания // Компьютерные инструменты в образовании. 2016. № 1. С. 17–23.
10. Classification: Accuracy [Электронный ресурс]. Режим доступа: https://developers.google.com/machine-learning/crash-course/classification/accuracy, свободный. Яз. англ. (дата обращения 20.03.2018).
11. Learned-Miller E., Huang G.B., RoyChowdhury A., Li H., Hua G. Labeled faces in the wild: a survey / In: Advances in Face Detection and Facial Image Analysis. Springer, 2016. P. 189–248. doi: 10.1007/978-3-319-25958-1_8
12. Каждая секунда на счету: почему скорость страницы должна стать вашим следующим центром внимания [Электронный ресурс]. Режим доступа: http://thewall.by/kazhdaya-sekunda-na-schetu-pochemu-skorost-stranicy-dolzhna-stat-vashim-sleduyushhim-centrom-vnimaniya, свободный. Яз. англ. (дата обращения 20.03.2018).

10.1016/j.imavis.2016.03.018
4. Casti S., Sorrentino F., Spano L.D., Scateni R. Click and share: A face recognition tool for the mobile community. *Proc. Int. Conf. on Image Processing, ICIP*, 2014, pp. 1952–1956. doi: 10.1109/ICIP.2014.7025391
5. Srirama S.N., Paniagua C., Flores H. Social group formation with mobile cloud services. *Service Oriented Computing and Applications*, 2012, vol. 6, no. 4, pp. 351–362. doi: 10.1007/s11761-012-0111-5
6. Lochner S.A. Saving face: regulating law enforcement's use of mobile facial recognition technology and Iris scans. *Arizona Law Review*, 2013, vol. 55, no. 1, pp. 201–233.
7. *Arrivals Smart Gate*. Available at: http://www.homeaffairs.gov.au/Trav/Ente/Goin/Arrival/Smartgateor-ePassport (accessed 20.03.2018).
8. Kukharev G.A., Kamenskaya E.I., Matveev Y.N., Shchegoleva N.L. *Methods for Face Image Processing and Recognition in Biometric Applications*. Ed. M.V. Khitrov. St. Petersburg, Politekhnika Publ., 2013, 388 p. (In Russian)
9. Ivanko D.V. Modeling of face recognition systems using mnemonic description of the model. *Computer Tools in Education*, 2016, no. 1, pp. 17–23. (In Russian)
10. *Classification: Accuracy*. Available at: https://developers.google.com/machine-learning/crash-course/classification/accuracy (accessed 20.03.2018).
11. Learned-Miller E., Huang G.B., RoyChowdhury A., Li H., Hua G. Labeled faces in the wild: a survey. In *Advances in Face Detection and Facial Image Analysis*. Springer, 2016, pp. 189–248. doi: 10.1007/978-3-319-25958-1_8
12. *Every second counts: why the speed of the page should be your next focus*. Available at: http://thewall.by/kazhdaya-sekunda-na-schetu-pochemu-skorost-stranicy-dolzhna-stat-vashim-sleduyushhim-centrom-vnimaniya (accessed 20.03.2018).

Авторы

Иванько Дмитрий Викторович – аспирант, Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация, Scopus ID: 56938960100, ORCID ID: 0000-0003-2347-5060, dmitriy_ivanko@yahoo.com

Authors

Dmitriy V. Ivanko – postgraduate, ITMO University, Saint Petersburg, 197101, Russian Federation, Scopus ID: 56938960100, ORCID ID: 0000-0003-2347-5060, dmitriy_ivanko@yahoo.com