УДК 004.056.53

Я.М. Жевандрова, А.А. Сыропятов, В.Д. Буряк

Одесский национальный политехнический университет, Одесса

КОМПЛЕКСНАЯ БИОМЕТРИЧЕСКАЯ АУТЕНТИФИКАЦИЯ ЛИЧНОСТИ

Надежность биометрических систем аутентификации, использующих несколько биометрических признаков, быстро возрастает. Целью исследования является поиск способа разработки мультибиометрической системы на портативном устройстве без использования специализированных считывателей. В качестве биометрических признаков выбраны лицо и отпечаток пальца, получаемые с помощью веб-камеры. При аутентификации используются технологии распознавания образов, компьютерного зрения и машинного обучения, а также дополнительная обработка изображения отпечатка пальца.

***Ключевые слова**: мультибиометрия, аутентификация, компьютерное зрение, обработка изображений, машинное обучение.*

Введение

Использование биометрических методов в области аутентификации и контроля доступа к информации в наше время получило широкое распространение. Анализ современного рынка показал, что биометрические средства защиты информации пользуются особым спросом и заняли достойное место благодаря высокой надежности аутентификации. Однако необходимо помнить о существующих уязвимостях данных систем.

Производители портативной техники (ноутбуки, телефоны, планшеты), в стремлении не отставать от научно-технического прогресса, массово интегрируют биометрические технологии в свои устройства. Заявленное высочайшее качество и надежность дешевых биометрических систем, интегрированных в портативную электронику, неоднократно опровергались. Не составит труда найти во Всемирной паутине видеоматериалы с наглядной демонстрацией обмана таких сканеров.

В данном случае целесообразно использовать дорогостоящие мультибиометрические системы, усложняющие процесс аутентификации, тем самым укрепляя надежность системы.

Прикладной областью является доступ к портативному устройству. Так как вся современная портативная техника оснащена камерами, были выбраны биометрические признаки – геометрия лица, а также рисунок отпечатка пальца ввиду высокой статистической достоверности.

Исходя из выбранной прикладной области, в мультибиометрической системе в качестве сканера биометрических параметров (лица и отпечатка пальца) используется обыкновенная веб-камера, что снижает затраты на специальное оборудование. Аутентификация осуществляется в виде поиска на видеопотоке заведомо хранимой в базе информации биометрических признаков.

Цель исследования и постановка задачи. Целью работы является разработка комплексной биометрической системы аутентификации на портативном устройстве без использования специализированных считывателей.

При аутентификации по геометрии лица стоит задача выбора алгоритма сравнения из тех, которые предоставляет библиотека компьютерного зрения OpenCV [1]. В случае дактилоскопической аутентификации (по отпечатку пальца) решается задача обработки изображения для возможности выделения особых точек, которые представляют собой конечные точки и точки ветвления [2] на папиллярном узоре, и сравнения с эталоном.

Основная часть

В данном случае OpenCV предоставляет выбор между вошедшими в него алгоритмами, а именно Eigenfaces, Fisherfaces и SURF (Speeded-Up Robust Features) [3]. Благодаря независимости от изменения условий освещенности и аффинным преобразованиям (масштабирование, перенос, поворот) в решении задачи идентификации лица было решено использовать алгоритм SURF [4].

Кроме того, был проведен эксперимент, в котором анализировалась эффективность предложенных алгоритмов идентификации лиц. Для сравнения эффективности использовались два тестовых набора: случай естественного и искусственного освещения. База данных в количестве десяти изображений лиц создавалась при естественном освещении. В качестве тестового набора были использованы по 3 видеозаписи, снятых при естественном и искусственном освещении. Каждая видеозапись содержит одну персону. Все алгоритмы идентификации принимали на вход одинаковый набор данных. Результаты работы алгоритмов на тестовых множествах с естественным и искусственным освещением представлены в табл. 1. Выбранный для решения задачи идентификации лица алгоритм SURF обладает лучшими показателями вероятностей верной и ложной идентификации среди рассмотренных алгоритмов на двух тестовых множествах.

Таблица 1

Результаты алгоритмов идентификации лиц на тестовом множестве

№	Вероятность верной идентификации			Вероятность ложной идентификации		
	SURF	Eigen Faces	Fisher Faces	SURF	Eigen Faces	Fisher Faces
Естественное освещение						
1	0,79	0,30	0,50	0,14	0,33	0,35
2	0,88	0,00	0,00	0,05	0,54	0,79
3	0,76	0,69	0,68	0,12	0,30	0,18
Искусственное освещение						
1	0,50	0,03	0,13	0,20	0,50	0,50
2	0,77	0,00	0,00	0,15	0,90	0,90
3	0,75	0,00	0,00	0,18	1,00	1,00

Отметим, что сумма вероятностей верной и ложной идентификации не равна единице из-за отдельных кадров без достаточной фокусировки, на которых алгоритм не выделил особых точек (ключевых точек). Ключевая точка изображения – существенно отличающаяся от основной массы точек (резкие перепады освещенности, углы и т.д.). Из формулы

$$\det(\mathrm{H}) = \frac{\partial^2 \mathrm{f}}{\partial \mathrm{x}^2} \cdot \frac{\partial^2 \mathrm{f}}{\partial \mathrm{y}^2} - \left(\frac{\partial^2 \mathrm{f}}{\partial \mathrm{x} \partial \mathrm{y}} \right),$$

где H – матрица Гессе [5], определитель матрицы Гессе для каждого пикселя изображения позволяет определить особые точки изображения. Матрица Гессе представляет собой квадратную матрицу, образованную вторыми частными производными функции. Детерминант матрицы достигает экстремума в точках максимального изменения градиента яркости.

Ключевая точка найдена в случаях, когда значение определителя превысило специально установленный порог, операция выполняется для каждого пикселя изображения.

Далее для каждой найденной особой точки вычисляется ориентация – преобладающее направление перепада яркости. Понятие ориентации близко к понятию направления градиента, но для определения ориентации особой точки применяется фильтр Хаара [4]. Выбор размеров фильтров и анализируемых окрестностей соответствует размеру области взятия вторых производных. Вокруг ключевой точки описывается прямоугольная область размером 20S, где S – масштаб, на котором получено максимальное значение детерминанта матрицы Гесса. Эта область разбивается на 16 квадрантов, одинаковых размеров. Прямоугольная область затем поворачивается в соответствии с ориентацией ключевой точки. На следующем шаге считаются оценки для каждого из 16-ти квадрантов области с помощью фильтров Хаара: $\sum \mathrm{dx}, \sum |\mathrm{dx}|, \sum \mathrm{dy}, \sum |\mathrm{dy}|$ – суммарные градиенты по квадранту и сумма модулей точечных градиентов. Размеры прямоугольной области, а также размеры фильтров Хаара зависят от размера области взятия вторых производных. В результате получается вектор из 64 чисел. Также, к описанию точки добавляется след матрицы Гёссе. Вектор и след матрицы вместе образуют дескриптор ключевой точки [4].

За счет использования вторых производных алгоритм SURF невосприимчив к перепадам яркости. Благодаря использованию разных размеров области взятия вторых производных и вычислению ориентации ключевых точек алгоритм становится инвариантен к изменению масштаба и повороту лица человека в плоскости изображения.

Исходя из прикладной области и использования веб-камеры в качестве считывателя биометрических параметров, возникает необходимость решить задачу улучшения качества изображения отпечатка. Для этого над изображением отпечатка пальца совершаются следующие операции:

Дебайеризация, дискретизация и ресайзинг – получение нужного разрешения и размера изображения, в данном случае 500dpi, 800×600; где дебайеризация – процесс трансляции матрицы первичных цветов Байера [6] в итоговое изображение, в котором содержится полная информация о цвете в каждом пикселе. Получение рисунка нужного разрешения в формате tiff реализовано в консольном фото−декодер dcraw [7] с флагами: –i (бикубическая интерполяция), –h (метод half) –T (формат изображения tiff).

Фильтрация. Изображение подвержено воздействию различных типов шумов, поэтому было принято решение на данном этапе работы системы воспользоваться фильтром Габора [8].

Для выделения границ и линий изображения отпечатка пальца используется сегментация. В результате исследования, был выбран метод Canny [9] для сегментации. Фактически это набор последовательно применяемых алгоритмов. Данный подход устойчивый к шуму и дает, как правило, лучшие результаты по сравнению с другими методами. Сравнение полученного образца отпечатка с эталонным осуществляется по методу выделения минуций (конечным точкам и точкам ветвления) [2].

Конечные точки (окончания выступов) – точки, в которых «отчетливо» заканчиваются папиллярные линии отпечатка. Точки ветвления – точки, в которых папиллярные линии раздваиваются.

Был проведен эксперимент по выделению особых точек на отпечатках пальцев. В первом случае метод выделения минуций был применен к изображениям, полученным с веб-камеры, без преобразований. Результаты показаны на рис. 1.

Во втором случае изображения подверглись преобразованиям, результат выделения минуций на преобразованных изображениях представлен на рис. 2. Видно, что количество выделяемых минуций после обработки заметно возросло, оказав положительное влияние на показатели надежности модуля сравнения отпечатков в составе мультибиометрической системы (рис. 3).

Рис. 1. Минуции на изображениях без обработки

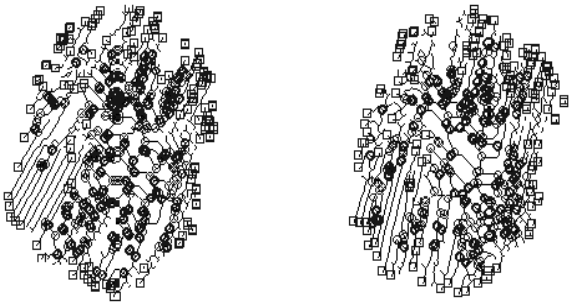

Рис. 2. Минуции обработанных изображений

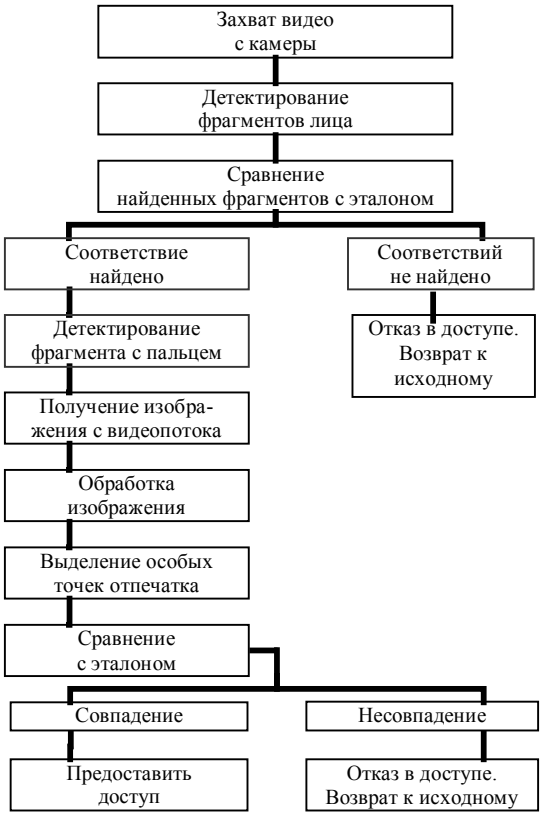

Рис. 3. Схема алгоритма мультибиометрической системы

Для программной реализации мультибиометрической системы были использованы следующие технологии разработки: язык программирования Python 2.7, библиотека компьютерного зрения OpenCV, консольный фото-декодер dcraw.

Из рис. 3 для покадрового выделения фрагмента лица и пальца на видео используется метод Виолы-Джонса [10], который в настоящее время является самым популярным методом для поиска объектов на изображении в реальном времени в силу своей скорости и эффективности.

Принципы, на которых основан метод:

Интегральное представление изображений [11] – матрица, совпадающая по размерам с исходным изображением. В каждом элементе ее хранится сумма интенсивностей всех пикселей, находящихся левее и выше данного элемента, что помогает быстро вычислить нужный объект.

Признаки Хаара – признаки цифрового изображения, используемые в распознавании образов, для поиска нужного объекта. Каждый признак представляет собой двоичную маску, т.е. черно-белое изображение. В стандартном методе Виолы-Джонса используются прямоугольные признаки, изображенные на рис. 4, они называются примитивами Хаара. Для описания объекта с достаточной точностью необходимо большее число признаков. Поэтому в методе Виолы-Джонса признаки Хаара организованы в каскадный классификатор.

В контексте алгоритма, имеется множество объектов (изображений), разделённых некоторым образом на классы.

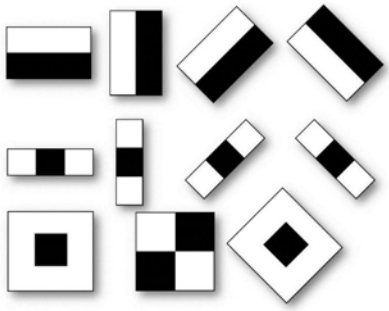

Рис. 4. Примитивы Хаара

Задано конечное множество изображений, для которых известно, к какому классу они относятся. Это множество называется обучающей выборкой. Выбор подходящих признаков на определенной части изображения при помощи Бустинга [12] (алгоритма AdaBoost) – это процедура последовательного построения композиции алгоритмов машинного обучения, когда каждый следующий алгоритм стремится компенсировать недостатки композиции всех предыдущих алгоритмов. Все признаки поступают на вход классификатора, возвращающего «истину» либо «ложь», каскады признаков используются для отбрасывания окон, где не найден объект.

В расширенном методе Виолы-Джонса, реализованном в библиотеке OpenCV, используются дополнительные признаки (рис. 5). Вычисляемое значение дополнительного признака $F=X-Y$, где X – сумма значений яркостей точек, закрываемых светлой частью признака, а Y – сумма значений яркостей точек, закрываемых темной частью признака. Признаки Хаара дают точечное значение перепада яркости по оси X и Y соответственно.

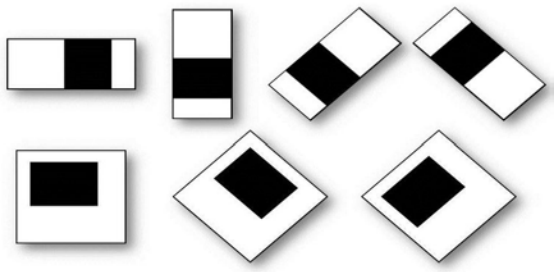

Рис. 5. Дополнительные признаки метода Виолы-Джонса

При обучении классификатора для надежного детектора потребовалось 3000 положительных примеров и столько же отрицательных. В эквиваленте видеосъемки с обычной для веб-камеры частотой до 30 кадров в секунду для сбора обучающей выборки потребуется до двух минут съемки.

Надежность биометрических системы принято определять с помощью показателей FRR и FAR, где ошибка первого рода (FRR – False Rejection Rate) представляет вероятность ложного отказа в доступе пользователю, имеющему право доступа, и ошибка второго рода (FAR – False Acceptance Rate) – это вероятность ложного доступа, когда система ошибочно опознает чужого как своего. Экспериментально были определены данные показатели для отдельных модулей рассматриваемой системы.

Выводы

Рассмотренную мультибиометрическую систему аутентификации, использующую в качестве сканера биометрических параметров веб-камеру, можно считать надежной.

Принимая во внимание исследование алгоритмов, вошедших в систему, и проведя тестирование, получены следующие результаты надежности для идентификации лица FAR до 1% и FRR до 20% (с учетом неспособности системы выделить особые точки на недостаточно сфокусированных кадрах), а также FAR до 1% и FRR до 5% для отпечатка пальца.

На основании полученных значений критерий надежности для системы в целом является допустимым и может использоваться в любых портативных устройствах.

Список литературы

1. Bradski G. Learning OpenCV [Электронный ресурс] / G. Bradski, A. Kaebler. – 2008. – Режим доступа к ресурсу: http://www.cse.iitk.ac.in/users/vision/dipakmj/papers/OReilly%20Learning%20OpenCV.pdf.

2. Задорожный В.В. Идентификация по отпечаткам пальцев [Текст] / В.В. Задорожный // PC Magazine Russian Edition. – 2004. – №1. – С. 25-35.

3. Face Recognition with OpenCV. [Электронный ресурс]. – Режим доступа к ресурсу: http://docs.opencv.org/2.4/modules/contrib/doc/facerec/facerec_tutorial.html.

4. Bay. Speeded-up robust features (SURF) / Herbert, Andreas Ess, Tinne Tuytelaars, Luc Van Gool // Computer vision and image understanding 110, no. 3 – 2008. – P. 346-359.

5. Форсайт Д. Компьютерное зрение. Современный подход [Текст] / Д. Форсайт, Ж. Понс, М. Вильямс. – М.: Издательский дом "Вильямс", 2004. – 928 с.

6. Фильтр Байера [Электронный ресурс]. – Режим доступа к ресурсу: https://traditio.wiki/Фильтр_Байера.

7. Dave Coffin (2014). dcraw.c,v-complete unabridged RCS file. [Электронный ресурс]. – Режим доступа к ресурсу: http://www.cybercom.net/~dcoffin/dcraw/RCS/ dcraw.c,v.

8. Гонсалес Р. Цифровая обработка изображений / Р. Гонсалес, Р. Вудс. – М.: Техносфера, 2005. – 1072 с.

9. Canny John. A Computational Approach to Edge Detection / John Canny // IEEE Transactions on pattern analysis and machine intelligence. – 1986. – Vol.8, № 6. – P. 679-698.

10. Viola P. Robust real-time face detection / P. Viola, M.J. Jones // International Journal of Computer Vision. – 2004. – Vol. 57, no. 2. – P. 137-154.

11. Татаренков Д.А. Анализ методов обнаружения лиц на изображении [Текст] / Д.А. Татаренков // Молодой ученый. – 2015. – №4. – С. 270-276.

12. Бустинг [Электронный ресурс] – Режим доступа к ресурсу: http://machinelearning.ru/wiki/index.php?title= Бустинг.

Поступила в редколлегию 22.03.2016

Рецензент: д-р техн. наук, доц. В.Я. Чечельницкий, Одесский национальный политехнический университет, Одесса.

КОМПЛЕКСНА БІОМЕТРИЧНА АУТЕНТИФІКАЦІЯ ОСОБИСТОСТІ

Я.М. Жевандрова, А.А. Сироп'ятов, В.Д. Буряк

Надійність біометричних систем аутентифікації, що використовують кілька біометричних ознак, швидко зростає. Метою дослідження є пошук засобу розробки мультибіометричної системи на портативному пристрої без використання спеціалізованих зчитувачів. В ролі біометричних ознак обрані обличчя і відбиток пальця, одержувані за допомогою веб-камери. Під час аутентифікації використовуються технології розпізнавання образів, комп'ютерного зору і машинного навчання, а також додаткова обробка зображення відбитка пальця.

***Ключові слова**: мультибіометрія, аутентифікація, комп'ютерний зір, обробка зображень, машинне навчання.*

COMPOUND BIOMETRIC PERSONALITY AUTHENTICATION

Y.M. Zhevandrova, A.A. Syropyatov, V.D. Buryak

The reliability of biometric authentication systems which use multiple biometric features is increasing rapidly. The aim of the research is to find ways for development of multi-biometric systems on a portable device without the use of specialized scanners. Face and fingerprint selected as biometric features which obtained by means of a webcam. Pattern recognition, computer vision, machine learning and additional fingerprint image processing are used for authentication.

***Keywords:** multi-biometrics, authentication, computer vision, digital image processing, machine learning.*