

УДК 004.056.53

СИСТЕМА КОМПЛЕКСНОЙ БИОМЕТРИЧЕСКОЙ АУТЕНТИФИКАЦИИ ЛИЧНОСТИ

Я. М. Жевандрова, Н. И. Кушниренко

Одесский национальный политехнический университет
Украина, г. Одесса
geva@list.ru

В системе биометрической аутентификации личности 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

Биометрические системы, обеспечивая уровень защиты выше, чем пароли или ПИН-коды, пользуются особым спросом в наше время. Целью работы является поиск способа разработки мультибиометрической системы на портативном устройстве без использования специализированных считывателей. Прикладной областью является доступ к портативному устройству с веб-камерой. Для покадрового выделения фрагмента лица и отпечатка пальца на видео используется метод Виолы–Джонса [1], который в настоящее время является самым популярным методом для поиска объектов на изображении в реальном времени в силу своей скорости и эффективности.

При аутентификации по геометрии лица стоит задача выбора алгоритма сравнения из тех, которые предоставляет библиотека компьютерного зрения OpenCV [2], а именно Eigenfaces, Fisherfaces и SURF (Speeded-Up Robust Features). Сравнение эффективности работы алгоритмов с использованием трех видеозаписей представлено в таблице.

Вероятность идентификации лиц разными алгоритмами на тестовом множестве с естественным освещением

№	Вероятность верной идентификации			Вероятность ложной идентификации		
	SURF	EigenFaces	FisherFaces	SURF	EigenFaces	FisherFaces
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

Отметим, что сумма вероятностей верной и ложной идентификации не равна единице из-за наличия отдельных кадров без достаточной фокусировки. Благодаря лучшим показателям и аффинным преобразованиям (масштабирование, перенос, поворот) в решении задачи идентификации лица было решено использовать алгоритм SURF.

В случае дактилоскопической аутентификации (по отпечатку пальца) решается задача обработки изображения для возможности выделения особых точек, которые представляют собой конечные точки и точки ветвления [3] на папиллярном узоре, и сравнения с эталоном. Для этого над изображением отпечатка пальца совершаются следующие операции.

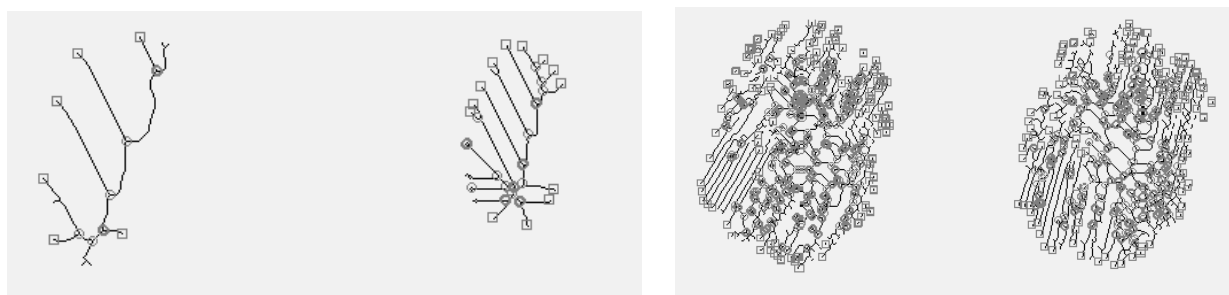
Для получения нужного разрешения и размера изображения, в данном случае 500 dpi, 800×600 используется дебайеризация, дискретизация и ресайзинг; где дебайеризация — процесс трансляции

матрицы первичных цветов Байера в итоговое изображение, в котором содержится полная информация о цвете в каждом пикселе. Получение рисунка нужного разрешения в формате tiff реализовано в консольном фото-декодере dcam (свободная компьютерная программа для преобразования файлов) с флагами: $-i$ (бикубическая интерполяция), $-h$ (метод half) $-T$ (формат изображения tiff).

Так как изображение подвержено воздействию шумов различных типов, то на данном этапе работы системы для фильтрации используется фильтр Габора.

Для выделения границ и линий изображения отпечатка пальца используется сегментация. В результате исследования было принято решение использовать метод Canny. Фактически это набор последовательно применяемых алгоритмов. Данный подход устойчив к шуму и дает, как правило, лучшие результаты по сравнению с другими методами.

Был проведен эксперимент по выделению особых точек. Результаты показаны на рисунке, где слева — минущии, выделенные на изображениях отпечатков пальцев, полученных с веб-камеры, без преобразований, справа — изображения, подвергнутые преобразованиям.



Выделение особых точек на изображениях

Очевидно, что количество выделяемых минущий после обработки заметно возросло, что оказывает положительное влияние на показатели надежности модуля сравнения отпечатков в составе мультибиометрической системы.

Таким образом, рассмотренную мультибиометрическую систему аутентификации, использующую в качестве сканера биометрических параметров веб-камеру, можно считать надежной. Приняв во внимание исследование алгоритмов, вошедших в систему, и проведя тестирование, мы получили следующие результаты надежности: при идентификации лица FAR составляет до 1% и FRR — до 20% , а при идентификации отпечатка пальца FAR составляет до 1% и FRR — до 5%. На основании полученных значений критерий надежности для системы в целом является допустимым и может использоваться в любых портативных устройствах.

ИСПОЛЬЗОВАННЫЕ ИСТОЧНИКИ

1. Viola P., Jones M.J. Robust real-time face detection // International Journal of Computer Vision.— 2004.— Vol. 57, no. 2. — P. 137–154.
2. Bradsky G., Kaehler A. Learning OpenCV — O'Reilly, 2008. — 557p.
3. Задорожный В.В. Идентификация по отпечаткам пальцев // PC Magazine Russian Edition – 2004.— N 1 – P. 25–35.

Y. M. Zhevandrova, N. I. Kushnirenko

Multi-biometric personality authentication system

Biometric personality authentication systems based on several biometric features are widely used in modern portable equipment. 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.*