

УДК 004.4

**РАЗРАБОТКА БИОМЕТРИЧЕСКОЙ СИСТЕМЫ
ИДЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЯ****Мишунина Надежда Олеговна**

старший преподаватель
Казахский агротехнический университет им. С Сейфуллина
Астана (Казахстан)

author@apriori-journal.ru

Аннотация. В статье кратко описаны результаты построения биометрической системы идентификации пользователя по его изображению, полученному через веб-камеру. Созданная система является синтезом двух направлений: компьютерного зрения и информационной безопасности.

Ключевые слова: идентификация; распознавание образов; биометрия, компьютерное зрение.

DEVELOPMENT BIOMETRIC SYSTEMS IDENTIFY USERS**Mishunina Nadezhda Olegovna**

senior lecturer
S. Seyfullin Kazakh Agro Technical University, Astana (Kazakhstan)

Abstract. The article briefly describes the results of the construction of a biometric identification system by using image obtained via webcam. The developed system is a synthesis of two directions: computer vision and information security.

Key words: identification; recognition of images; biometrics; computer sight.

В поисках новых методов защиты разработчики всё чаще обращают своё внимание на биометрические системы. Биометрические системы распознают людей на основе их анатомических особенностей (отпечатков пальцев, образа лица, рисунка линий ладони, радужной оболочки, голоса) или поведенческих черт (подписи, походки). При грамотной реализации в соответствующих приложениях биометрические системы обеспечивают высокий уровень защищенности.

Цель данной работы – построение биометрической системы идентификации пользователя, основанной на распознавании лиц пользователей компьютерных систем. Система представлена синтезом двух направлений: компьютерного зрения и информационной безопасности.

Как научная дисциплина, компьютерное зрение относится к теории и технологии создания искусственных систем, которые получают информацию из изображений. Видеоданные могут быть представлены множеством форм, таких как видеопоследовательность, изображения с различных камер или трехмерными данными, например с устройства Kinect или медицинского сканера.

Как технологическая дисциплина, компьютерное зрение стремится применить теории и модели компьютерного зрения к созданию систем компьютерного зрения. Примерами применения таких систем могут быть:

- 1) системы управления процессами (промышленные роботы, автономные транспортные средства);
- 2) системы видеонаблюдения;
- 3) системы организации информации (например, для индексации баз данных изображений);
- 4) системы моделирования объектов или окружающей среды (анализ медицинских изображений, топографическое моделирование);
- 5) системы взаимодействия (например, устройства ввода для системы человеко-машинного взаимодействия);

- 6) системы дополненной реальности;
- 7) вычислительная фотография, например, для мобильных устройств с камерами.

Компьютерное зрение производит среднеуровневый анализ данных, заключающийся в выделении на изображении каких-либо объектов, и измерении их параметров [1].

Комбинируемая защита, состоящая из аутентификации пользователя по логину и паролю и идентификации по биометрическим показателям позволяет в разы увеличить безопасность компьютерной системы от несанкционированного доступа.

Можно выделить следующие задачи, решаемые программой идентификации:

- обеспечение доступа авторизованным пользователям к операционной системе для работы на ПК средствами визуального определения личности по фронтальному изображению с потока видеокamеры;
- создание и удаление новых пользователей системы;
- ведение учёта длительности сеансов зарегистрированных пользователей;
- ведение и поддержка журнала попыток авторизации, включая данные о результатах, фотоснимки авторизующихся пользователей и данные о времени;
- возможность авторизации с использованием пароля в случае недоступности видеокamеры или критического изменения внешности пользователя.

Следует подчеркнуть, что необходимость усиления защиты в некоторых случаях требует от разработчиков создания достаточно сложных систем с учётом биометрических показателей – отпечатков пальцев, сканирования сетчатки глаза, внешнего вида пользователя. Последний из перечисленных выбран для создаваемой программы благодаря следующим качествам:

- веб-камера установлена на 95 % переносных и около 60 % стационарных компьютеров;
- её стоимость, колеблющаяся в среднем показателе в пределах 20-40 долларов, делает девайс доступным как в личных целях, так и в корпоративных. В сравнении со съёмщиком отпечатков пальцев или лазерными сверхточными устройствами для идентификации по сетчатке глаза стоимость системы снижается многократно;
- использование не требует специфических мер, реагентов, температур, предварительной подготовки или каких-либо непривычных пользователю процедур;
- отличные показатели производительности в рамках компьютерных ресурсов – оперативной памяти и процессорных тактов даже на слабых компьютерах;
- и, наконец, высокий процент точности распознавания пользователя.

Входными данными проекта являются: логин пользователя, фронтальные фотографии лица и пароль. Логин и пароль могут быть введены на любом языке, поддерживаемом кодировкой UTF-8. Фотографии не ограничены по размеру или разрешению. Однако, для корректности работы программы рекомендуется выбирать снимки с большим разрешением и, желательно, крупным планом лица пользователя. Также играет существенную роль количество фотографий – от 1 до 16. Предоставив большее количество снимков с разным углом наклона и освещения, возрастает степень распознавания пользователя.

При разработке программы использовалась библиотека OpenCV (англ. Open Source Computer Vision Library, библиотека компьютерного зрения с открытым исходным кодом). OpenCV – это библиотека алгоритмов компьютерного зрения, обработки изображений и численных алгоритмов общего назначения с открытым кодом. Реализована на C/C++, также разрабатывается для Python, Java, Ruby, Matlab, Lua и других язы-

ков. Может свободно использоваться в академических и коммерческих целях – распространяется в условиях лицензии BSD [2].

Для поиска объекта на изображении (например, лица), а также проверки этого объекта на принадлежность некоторому классу (верификация, распознавание эмоций, пола по лицу) может быть использован оператор Local Binary Patterns (LBP) [3].

Оператор LBP впервые был предложен Т. Оjala в 1996 году. Он представляет собой эффективный оператор, в котором каждый пиксель изображения значитсся в виде бинарного числа, зависящего от интенсивностей соседних пикселей изображения.

Как правило, система распознавания лиц представляет собой программно-аппаратный комплекс для автоматической верификации или идентификации личности по цифровому изображению (фотографии или кадру видеопоследовательности).

В процессе распознавания лиц возникает ряд сложностей, связанных с изменением условий освещения, вращением головы, возрастными изменениями и проч. Можно выделить следующие основные этапы процесса верификации и идентификации:

- регистрация и нормализация изображения;
- выбор признаков;
- вычисление меры близости;
- построение решающего правила.

Применяя оператор LBP к каждому пикселю изображения, мы можем построить гистограмму, в которой каждому равномерному коду локальных бинарных шаблонов (ЛБШ) соответствует отдельный столбец. Также имеется еще один дополнительный столбец, который содержит информацию обо всех неравномерных шаблонах.

Изображения лиц могут рассматриваться как набор всевозможных локальных особенностей, которые хорошо описываются с помощью локальных бинарных шаблонов. Однако гистограмма, построенная для

всего изображения в целом, кодирует лишь наличие тех или иных локальных особенностей, но при этом не содержит никакой информации об их расположении на изображении. Для учета такого рода информации изображение разбивается на подобласти, в каждой из которых вычисляется своя гистограмма ЛБШ. Путем конкатенации этих гистограмм может быть получена общая гистограмма, учитывающая как локальные, так и глобальные особенности изображения [4-5].

Приложение было разработано на языке программирования java с использованием виртуальной машины JVMJava 7.

Написание исходного кода, отладка приложения, тестирование и упаковка исполняемого модуля происходили с использованием EclipseKepler.

Основное рабочее окно программы имеет три вкладки: Тестирование, Пользователи и Авторизации (рисунок 1).



Рис. 1. Главное окно на вкладке тестирование

На первой вкладке размещаются все компоненты, необходимые для тестирования программы на распознавание уже зарегистрированного пользователя. Выпадающий список камер позволяет выбрать одну из имеющихся в системе, а также показывает, какая именно сейчас используется программой. Кнопка «Распознать с изображения» даёт возможность провести попытку распознавания не с потока кадров видеокамеры, а с выбранного пользователем изображения. Нажатие на неё автоматически приводит к открытию файлового диалога. Кнопка «Сохранить кадр» позволяет записать текущий кадр в формате изображения jpgv выбранном пользователем каталоге. Чекбокс «Отмечать лица в кадре» отвечает за необходимость отрисовки прямоугольников вокруг лиц, найденных в кадре видеопотока или загруженного изображения. Чекбокс «Сглаживать изображения в кадре» вызывает сглаживание картинки, что преимущественно важно для изображений с «пиксельным шумом».

На вкладке «Пользователи» располагаются компоненты работы с пользователями. Таблица, отображающая все сведения пользователей: логин, фронтальные изображения, доступ к паролю и дату последней авторизации. Справо от таблицы находится панель управляющих элементов, с помощью которых можно добавить нового пользователя, удалить существующего или всех. А также – панель аватара – увеличенного изображения с кнопками «Добавить фото» и «Удалить фото» (рисунок 2).

Вкладка «Авторизации» предоставляет доступ к таблице пользователей, которые пытались авторизоваться. Если пользователь зарегистрирован в программе, то поле логина заполняется его данными. Также сохраняется фотоснимок – кадр с видеопотока, который был использован при распознавании и помещается во второй столбец таблицы. Результат выводится в третий столбец в виде двух определений «авторизован» или «неавторизован». Последние два столбца отведены для данных о начале сеанса и завершении. На вкладке для удобства работы

помещены компоненты поиска, позволяющие делать фильтрацию по логину или времени авторизации (рисунок 3).

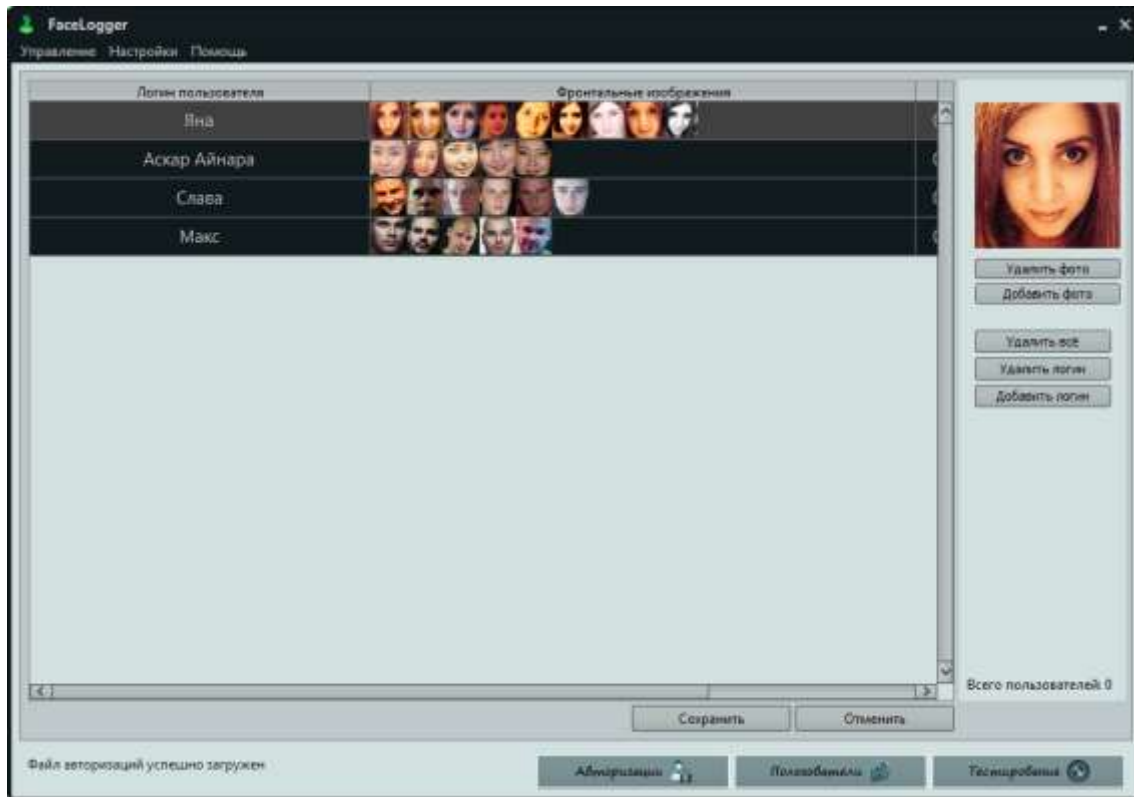


Рис. 2. Главное окно на вкладке пользователи

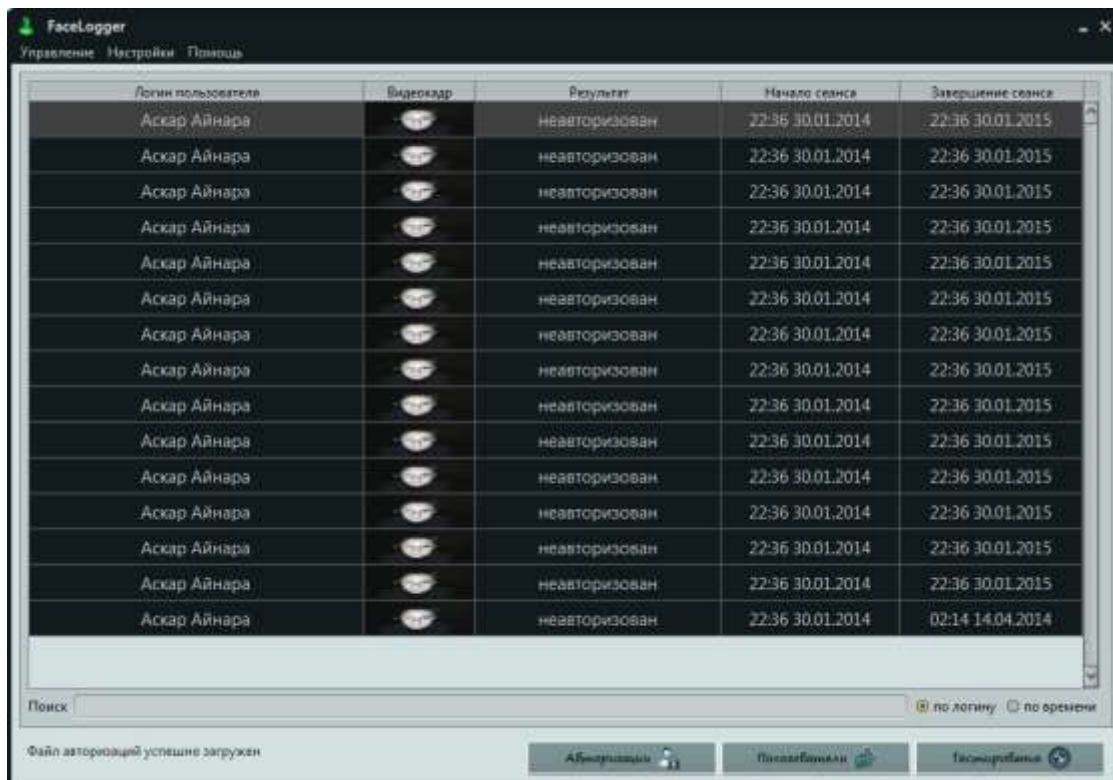


Рис. 3. Главное окно на вкладке Авторизации

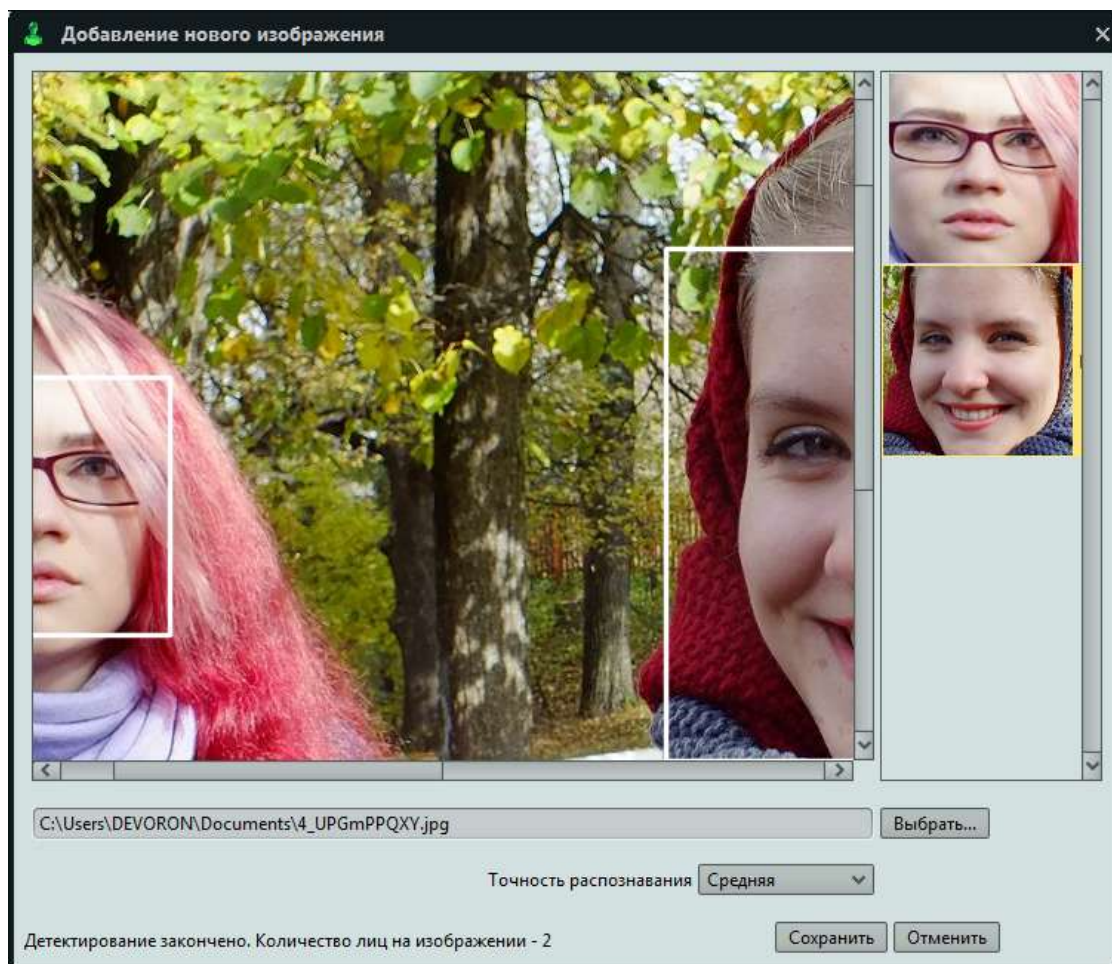


Рис. 4. Диалог добавления нового изображения

Диалоговое окно «Добавление нового изображения» содержит элементы, упрощающие действия по добавлению фронтальных изображений: кнопку «Выбрать» и текстовое поле, в котором отображается путь к изображению, панель на которой отрисовывается выбранное изображение с найденными на нём лицами, выделенными прямоугольниками и дублированными в список слева, для точного выбора конкретного лица. Также там находится выпадающий список, определяющий точность нахождения лица на изображении с четырьмя вариациями: «Низкая», «Средняя», «Высокая» и «Очень высокая». Результаты работы в виде текстового сообщения отображаются снизу слева, а конечный выбор осуществляется нажатием кнопки «Сохранить» или «Отменить» (рисунок 4).

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Форсайт Д.А., Понс Д. Компьютерное зрение. Современный подход. М.: Издательский дом «Вильямс», 2004. 928 с.
2. Bradsky G., Kaehler A. Learning OpenCV – O'Reilly. 2008. 580 p.
3. Ojala T., Pietikäinen M., Harwood D. A Comparative Study of Texture Measures with Classification Based on Feature Distributions // Pattern Recognition. V. 29. P. 51-59.
4. Maturana D., Mery D., Soto A. Face Recognition with Local Binary Patterns, Spatial Pyramid Histograms and Naive Bayes Nearest Neighbor classification // Proc. of the XXVIII International Conference of the Chilean Computer Science Society. IEEE CS Society. 2009. 202 p.
5. Shan C., Gong S., McOwan P.W. Facial expression based on Local Binary Patterns: A comprehensive study. Image and Vision Computing. 2009. 32 p.