ИНФОРМАТИКА. ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА. УПРАВЛЕНИЕ

УДК 519.7
MSC 03B70; 68T27; 68T30
DOI:10.35330/1991-6639-2020-4-96-5-10

ПРИМЕНЕНИЕ НЕЙРОСЕТЕВОГО ПОДХОДА ДЛЯ РЕШЕНИЯ ЗАДАЧИ АУТЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЯ

Л.А. ЛЮТИКОВА, А.С. ИБРАГИМ

Институт прикладной математики и автоматизации –
филиал ФГБНУ «Федеральный научный центр
«Кабардино-Балкарский научный центр Российской академии наук»
360000, КБР, г. Нальчик, ул. Шортанова, 89 А
E-mail: ipma@niipma.ru

Одним из эффективных методов обеспечения информационной безопасности на сегодняшний день является построение эффективных процедур аутентификации пользователей. Для успешного решения задачи ИБ необходим комплексный подход к идентификации пользователей. Одним из таких направлений является сбор и обработка биометрических данных о конкретном пользователе. Применение нейросетевого подхода обеспечивает как достаточно высокий уровень распознавания пользователей, так и достаточно удобную алгоритмическую реализацию.

В результате практического эксперимента на тестовых примерах выявлено, что предложенная методика использования нейронных сетей является эффективной, защищенной, повышает надежность распознавания и рекомендуется для внедрения на малых предприятиях.

Ключевые слова: нейронные сети, распознавание лица, распознавание жестов, метод Виолы – Джонса, признаки Хаара, корректирующие алгоритмы.

Введение

В данной работе использованы методики по распознаванию лица и распознаванию жестов пользователей для простых систем с недорогой аппаратурой, которые можно установить на малом предприятии, не требующие больших материальных вложений.

Идентификация по одному критерию может быть неточной в силу помех или ошибок распознавания. Поэтому необходимо располагать дополнительным, независящим от первого, критерием распознавания. При распознаваниях лица помехами могут служить плохая освещенность и блики, поэтому наряду с распознаванием лица нами используется распознавание жестов.

Распознавание лица

Реализацию идеи по распознаванию лица разделим на 3 этапа:

– обнаружение лица и сбор данных;

– обучение распознавателя;

– распознавание лица.

Для реализации этой идеи нами будет использоваться библиотека алгоритмов изображений, компьютерного зрения и численных алгоритмов общего назначения с открытым кодом OpenCV, программная реализация будет выполнена на языке Python версии 3 в среде разработки Visual Studio Code.

Наиболее распространенным способом обнаружения лица (или любых других объектов) является метод Виолы – Джонса, основанный на классификаторе каскадов Хаара. Рассмотрим метод Виолы – Джонса более подробно. Метод Виолы – Джонса – это алгоритм, предложенный Паулем Виолой и Майклом Джонсом в 2001 году, с помощью которого можно обнаружить объекты на изображениях в режиме реального времени [7]. В ос-

нове метода лежит использование технологии скользящего окна, представляющей собой рамку, по размеру меньшую, чем исходное изображение, которая двигается с некоторым шагом по изображению и на основании каскадов слабых классификаторов определяет, есть ли в рамке лицо. Метод скользящего окна часто применяют во многих задачах компьютерного зрения и распознавания объектов.

При практическом использовании скорость работы алгоритма обучения отходит на второй план, важнее скорость обработки алгоритма распознавания. У метода Виолы – Джонса можно выделить такие преимущества, как:

- возможность обнаружения нескольких лиц на изображении;
- применяемые простые классификаторы позволяют существенно увеличить скорость обработки и применять этот метод в видеопотоке.

Признаки класса

В расширенном методе Виолы – Джонса, который применяется в библиотеке OpenCV, признаки Хаара организованы в каскадный классификатор и используются дополнительные признаки, изображенные на рисунке.

По расширенным признакам намного легче определяется точечное значение перепада яркости по оси X и Y соответственно. Таким образом, набор двух смежных прямоугольников, находящихся выше глаз и на щеках, будет являться общим признаком Хаара для распознавания лиц. Значение признака будет вычисляться по формуле

$$F=X–Y,$$

где X – сумма значений яркостей точек, закрываемых светлой частью признака, а Y – сумма значений яркостей точек, закрываемых темной частью признака.

Обучение

Общая схема алгоритма обучения представлена следующим образом. Имеется тестовая выборка изображений. Размер тестовой выборки – около 10 000 изображений. Цвета для алгоритма не нужны, он работает в оттенках серого цвета.

При размере тестового изображения 24 на 24 пикселя количество конфигураций одного признака – около 40 000 (зависит от минимального размера маски). Современная реализация алгоритма использует порядка 20 масок. Для каждой маски каждой конфигурации тренируется такой слабый классификатор, который дает наименьшую ошибку на всей тренировочной базе. Он добавляется в базу данных, представляющую собой лица пользователей.

Таким образом, алгоритм обучается. И на выходе алгоритма получается база данных из T слабых классификаторов [1,2].

Для выполнения работы алгоритма необходимо заранее подготовить тестовую выборку из l изображений, содержащих искомый объект, и n – не содержащих. Общее количество тестовых изображений составит $n=l+m$. $X=\{x_1, x_2, \dots, x_n\}$, где X – множество всех тестовых изображений, где для каждого заранее известно, присутствует искомый объект или нет, и отражено во множестве Y: $Y=\{y_1,y_2,\dots,y_n\}$, где $y_j=\{1$, объект присутствует на изображении $x_i 0$, иначе под признаком j будем понимать структуру вида $J=\{$маска, положение, размер$\}$.

Задача сводится к формальной постановке распознавания по прецедентам [3].

Распознавание

После обучения на тестовой выборке имеется обученная база знаний из T классификаторов. Для каждого классификатора известны: признак Хаара, использующийся в этом классификаторе, его положение внутри окна размером 24x24 пикселя и значение порога E.

На вход алгоритму поступает изображение *I (r,c)* размером *W x H*, где *I(r,c)* – яркостная составляющая изображения. Результатом работы алгоритма служит множество прямоугольников *R(x, y, w, h),* определяющих положение лиц в исходном изображении. Алгоритм сканирует изображение *I* на нескольких масштабах, начиная с базовой шкалы: размер окна 24x24 пикселя и 11 масштабов, при этом каждый следующий уровень в 1.25 раза больше предыдущего.

Для обучения классификатора изначально требуется большое количество положительных изображений (изображений лиц) и неподходящих изображений (изображений без лиц). Эту задачу реализует OpenCV со встроенным тренером для обучения и детектором для распознавания. Сам классификатор создавать необязательно, в OpenCV поддерживается множество классификаторов для глаз, лица, улыбки.

Заключительным этапом нашего исследования является распознавание. Лицо, попадающее в камеру, подвергается обработке, если классификатор, обученный ранее, распознает пользователя, то возвращает свой идентификатор и индекс, показывающий, насколько уверен в этом признаке распознаватель.

Вторым этапом реализации поставленной нами цели является построение модели системы распознавания жестов.

Этот этап реализации мы будем использовать как средство аутентификации пользователей на заявленный идентификатор лица. Идея состоит в том, чтобы программа из видеопотока выбрала жест пользователя, распознала его и на основании результата распознавания предоставила или, наоборот, закрыла доступ пользователю, предварительно распознав лицо.

Эта задача требует достаточно высоких вычислительных ресурсов – жест руки снимается на видео и затем видеосигнал анализируется сложными алгоритмами, требующими значительных производительных мощностей. Эту задачу можно представить в виде подзадач, последовательное решение которых приведет к положительному результату и высокому уровню идентификации.

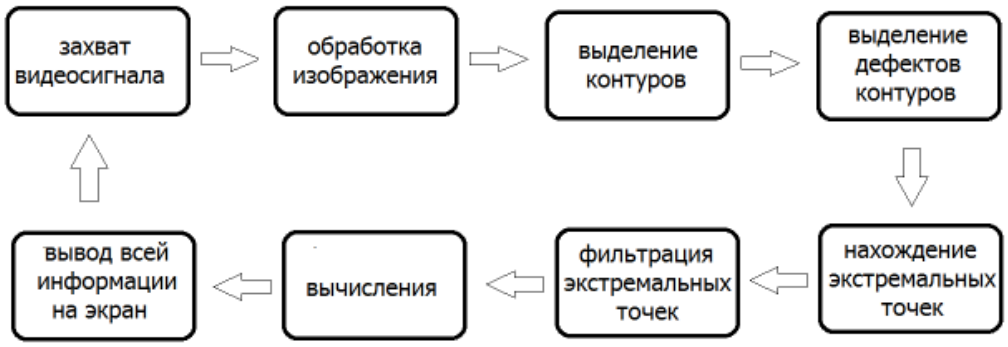

Рис. 1. *Поэтапное представление распознавания жестов*

Сначала программа должна получить видеосигнал с камеры и выделить из него одно изображение. Все остальные действия ведутся над анализом этого изображения, и после завершения всех процедур программа возвращает результат и захватывает новое изображение. Следующий после захвата изображения этап – его редактирование.

Программа должна максимально упростить себе задачу анализа: изображение должно быть максимально сжато по разрешению и не должно содержать лишних цветов. В данном случае нужно произвести пороговое преобразование в бинарный вид, так как будут использоваться именно бинарные методы. Далее программа должна выделить необходимые контуры изображения с помощью алгоритмов компьютерного зрения и найти их дефекты.

Далее нужно найти и отфильтровать так называемые экстремальные точки – они содержат большинство информации об объекте. Затем, исходя из положения этих точек,

нужно произвести необходимые вычисления и сделать вывод о том, какой именно жест демонстрируется. Также вся графическая информация должна быть показана на экране. После всех этих действий цикл следует повторить.

Первым этапом является захват камерой изображения и вывод его на экран [6].

Получив необходимый результат, представленный программой в качественном двоичном изображении силуэта руки, следует приступить к анализу изображения, который будет представлять собой массив из черных и белых пикселей [5]. Алгоритм представляет собой решение двух задач:

1. Структурирование массива пикселей.
2. Сравнение полученного массива с заданной константой.

При совпадении блока данных с константой система вернет определенный результат, в обратном случае появится сообщение об ошибке и несовпадении с заданной константой.

Построение математической модели коррекции алгоритмов

Для более точного распознавания как лиц, так и жестов можно использовать не один, а несколько алгоритмов, и на каждом наборе данных выбирать тот, который работает более точно. Для этого необходимо предложить метод для выбора конкретного алгоритма на заданном наборе данных [2,4].

Формальная постановка выглядит следующим образом: рассматривается ряд алгоритмов $A_1, A_2, \dots, A_n$, дающих некоторые решения задачи распознавания лиц и жестов.

Пусть $X = \{x_1, x_2, \dots, x_m\}$, множество признаков для распознавания лиц и жестов $x_i \in \{0,1, \dots, k_i - 1\}$, где $k_i \epsilon [2 \dots N], N \epsilon Z$–; $Y = \{y_1, y_2, \dots, y_l\}$ – множество распознаваемых объектов; $A = \{A_1, A_2, \dots, A_n\}$ – множество алгоритмов $a_j(X_i, y_i) \in \{0,1\}$; $i = 1,2, \dots, l; j = 1,2, \dots, n$ – качество работы алгоритма на заданном наборе признаков $X_i = \{x_1(y_i), x_2(y_i), \dots, x_m(y_i)\}, i = 1,2, \dots, l$:

$$a_j(X_i, y_i) = \begin{cases} 1, & A_j(X_i) = y_i \\ 0, & A_j(X_i) \neq y_i \end{cases}, \; i = 1,2, \dots, l, \; j = 1,2, \dots, n,$$

т.е. результат работы алгоритма на заданном наборе признаков оценивается в рамках булевой алгебры:

1 – алгоритм A_j распознал объект y_i по заданным признакам X_i,

0 – алгоритм A_j не распознал объект y_i по заданным признакам X_i.

$$\mathrm{A'}_i = \{a_i(y_1), a_i(y_2)), \dots, a_i(y_l)\}, i = 1,2, \dots, n.$$

Некоторые объекты не распознаются ни одним из рассматриваемых алгоритмов, т.е.

$$\exists\, i \in [1 \dots l], \mathrm{y}_i \in Y \mid A_j(X_i) \neq y_i, j \in [1 \dots n],$$
$$\exists\, \mathrm{y}_i \in Y \mid A_1(X_i) \neq y_i, A_2(X_i) \neq y_i, \dots, A_n(X_i) \neq y_i, \;\; i = 1,2, \dots, l\,.$$

Найти $A_{n+1}(X_i) | \, A_{n+1}(X_i) = y_i$ и $A_{n+1}(X) | \, A_{n+1}(X) = Y$.

Будем говорить, что алгоритм корректен на множестве $\{y_1, y_2, \dots, y_l\}$, $y_i \in Y$ если $\forall\, y_i \in \{y_1, y_2, \dots, y_l\} : a_j(X_i, y_i) = 1$. Иными словами, алгоритм является корректным на том множестве объектов, которые он правильно распознает [1, 3]. Назовем $\mathrm{A}_j{}'$ совокупностью решающих правил, которые алгоритм распознает, $\overline{A'_j}$ – совокупностью решающих правил, которые алгоритм не распознает:

$\mathrm{A}'_j = \; \&_{i=1}^{l} \, (\&_{j=1}^{m} x_j(y_i,) \to y_i)$ когда $a_j(X_i, y_i) = 1$,

$\overline{A'_j} = \&_{i=1}^{l} \, (\&_{j=1}^{m} x_j(y_i,) \to y_i)$ когда $a_j(X_i, y_i) = 0$,

выразим импликацию и получим следующие выражения:

$A'_j = \ \&_{i=1}^{l} (\vee_{j=1}^{m} \overline{x_j(y_i,)} \vee y_i)$ когда $a_j(X_i, y_i) = 1$,
$\overline{A'_j} = \&_{i=1}^{l} (\&_{j=1}^{m} \overline{x_j(y_i,)} \vee y_i)$ когда $a_j(X_i, y_i) = 0$,

Вся исследуемая предметная область может быть представлена в виде:

$$\&_{j=1}^{m} x_j(y_i) \to y_i, \ \ i = 1, \dots, l, \ \ x_j(y_i) \in \{0,1,,k-1\}.$$

Выводы

В качестве базовых критериев биометрической идентификации пользователей выбраны характеристики:

- распознавание лица;
- распознавание жестов.

В результате практического эксперимента на тестовых примерах выявлено, что предложенная методика использования нейронных сетей является эффективной, защищенной, повышает надежность распознавания и рекомендуется для внедрения на малых предприятиях.

Реализация систем распознавания пользователей по двум критериям, а также использование корректирующих алгоритмов позволит увеличить надежность аутентификации пользователей.

ЛИТЕРАТУРА

1. *Журавлёв Ю.И.* Об алгебраическом подходе к решению задач распознавания или классификации // Проблемы кибернетики. 1978. Т. 33. С. 5-68.

2. *Шибзухов З.М.* Корректные операции агрегирования с алгоритмами // Распознавание образов и анализ изображений. 2014. Т. 24. № 3. С. 377-382.

3. *Тимофеев А.В., Лютикова Л.А.* Развитие и применение многозначных логик и сетевых потоков в интеллектуальных системах // Труды СПИИ РАН. 2005. Вып. 2. С. 114-126.

4. *Лютикова Л.А.* Моделирование и минимизация баз знаний в терминах многозначной логики предикатов. Нальчик: Препринт, 2006. 33 с.

5. *Пол Д., Макуорт А., Гобель Р.* Вычислительный интеллект. Логический подход. Нью-Йорк: Издательство Оксфордского университета, 1998.

6. *Люгер Дж. Ф.* Искусственный интеллект: структуры и стратегии для комплексного решения проблем. 5-е издание. Изд-во «Бенджамин Каммингс», 2004. С. 720.

7. *Нильсон Нильс Ж.* Искусственный интеллект: новый синтез. Изд. Моргана Кауфмана, 1998.

REFERENCES

1. Zhuravlev Yu.I. *Ob algebraicheskom podkhode k resheniyu zadach raspoznavaniya ili klassifikatsii* [On an algebraic approach to solving problems of recognition or classification] // *Problemy kibernetiki* [Problems of Cybernetics]. 1978. Vol. 33. Pp. 5-68.

2. Shibzukhov Z.M. *Korrektnyye operatsii agregirovaniya s algoritmami* [Correct Aggregation Operations with Algorithms] // *Raspoznavaniye obrazov i analiz izobrazheniy* [Pattern Recognition and Image Analysis]. 2014. Vol. 24. No. 3. Pp. 377-382.

3. Timofeev A.V., Lyutikova L.A. *Razvitiye i primeneniye mnogoznachnykh logik i setevykh potokov v intellektual'nykh sistemakh* [Development and application of multivalued logics and network flows in intelligent systems] // Proceedings of SPII RAS. 2005. Vol. 2. Pp. 114-126.

4. Lyutikova L.A. *Modelirovaniye i minimizatsiya baz znaniy v terminakh mnogoznachnoy logiki predikatov* [Modeling and minimizing knowledge bases in terms of multivalued predicate logic]. Nalchik: Preprint, 2006. 33 p.

5. Poole David, Mackworth Alan & Goebel Randy. Computational Intelligence. A Logical Approach. New York: Oxford University Press, 1998.

6. Luger George & Stubblefield William. Artificial Intelligence: Structures and Strategies for Complex Problem Solving. 5th ed. The Benjamin / Cummings Publishing Company, Inc., 2004. P. 720.
7. Nilsson Nils. Artificial Intelligence: A New Synthesis. Morgan Kaufmann Publishers, 1998.

APPLICATION OF A NEURAL NETWORK APPROACH TO SOLVING USER AUTHENTICATION PROBLEMS

L.A. LYUTIKOVA, A.S. IBRAGIM

Institute of Applied Mathematics and Automation –
branch of the FSBSE «Federal Scientific Center
«Kabardin-Balkar Scientific Center of the Russian Academy of Sciences»
360000, KBR, Nalchik, Shortanov street, 89 A
E-mail: ipma@niipma.ru

One of the most effective methods for ensuring information security today is the construction of effective user authentication procedures. To successfully solve the information security problem, an integrated approach to user identification is required. One of the ways is the collection and processing of biometric data about a specific user. The use of a neural network approach provides both a sufficiently high level of user recognition and a fairly convenient algorithmic implementation.

As a result of a practical experiment on test examples, it was revealed that the proposed method of using neural networks is effective, secure, increases the reliability of recognition and is recommended for implementation in small businesses.

Keywords: neural networks, face recognition, gesture recognition, Viola – Jones method, Haar features, corrective algorithms.

Работа поступила 04.08.2020 г.

Сведения об авторах:

Лютикова Лариса Адольфовна, к.ф.-м.н., зав. отделом «Нейроинформатика машинного обучения» Института прикладной математики и автоматизации – филиала Кабардино-Балкарского научного центра РАН.
360000, КБР, г. Нальчик, ул. Шортанова, 89 А.
Тел. 8-963-166-40-14.
E-mail: lylris@yndex.ru
Ибрагим Анзор Субхи, аспирант НОЦ КБНЦ РАН 2 года 09.06.01 – Информатика и вычислительная техника 05.13.06 – Автоматизация и управление технологическими процессами и производствами (ОФО).
360002, КБР, г. Нальчик, ул. Балкарова, 2
E-mail: asibragim@gmail.com

Information about the authors:

Lyutikova Larisa Adolfovna, Candidate of Physical and Mathematical Sciences, Head of the Department of Machine Learning Neuroinformatics of the Institute of Applied Mathematics and Automation, a branch of the Kabardino-Balkarian Scientific Center of the Russian Academy of Sciences.
360000, KBR, Nalchik, Shortanova street, 89 A.
Ph. 8-963-166-40-14.
E-mail: lylris@yndex.ru
Ibrahim Anzor Subhi, 2nd year post-graduate, Scientific-educational Center of Kabardino-Balkarian Scientific Center of RAS 09.06.01 - Informatics and computer technology 05.13.06 - Automation and control of technological processes and production (OFO).
360002, KBR, Nalchik, Balkarova street, 2
E-mail: asibragim@gmail.com