

И. С. Ризаев, Э. Г. Тахавова, М. П. Шлеймович

МЕТОДЫ ИДЕНТИФИКАЦИИ ПОДПИСИ ЧЕЛОВЕКА*Ключевые слова: подписи, идентификация, текстура, классификация, программирование.*

В статье исследуются методы и подходы идентификации подписей конкретных людей. Рассматриваются основные концепции и принципы, связанные с обработкой и анализом подписей, включая предобработку изображений, извлечение признаков и классификацию подписей. Указывается, что подпись является биометрическим признаком, который человек может использовать без необходимости запоминания паролей, или использования дополнительных устройств. Рассмотрены различные методы идентификации, например, методы, учитывающие форму, текстуру, а также структуру подписи, скорость и ускорение характеризует динамику подписей. В ряде случаев могут быть использованы методы машинного обучения. Показано, что каждый из этих подходов имеет свои преимущества и ограничения. Показано, что используются следующие методы идентификации подписей: метод сопоставления шаблонов (Template Matching); метод, основанный на извлечении признаков (Feature Extraction); метод, основанный на нейронных сетях. Приведены их характеристики, а также преимущества и недостатки этих методов. Для выделения признаков используется математическая модель классификации по методу Байеса, где используются вероятностные модели для определения класса объекта на основе его признаков. Для программной реализации используется язык программирования Python и OpenCV - библиотека компьютерного зрения с открытым исходным кодом. Показано, что использование библиотеки для получения подписи выполняется в следующей последовательности: загрузка изображения; обработка изображения; сегментация подписи и сохранение изображения. Для проверки результатов используется набор данных, содержащий образцы подписей различных людей. В процессе реализации программы производится предобработка изображений с использованием извлечения характеристик и обучение классификатора на основе байесовского подхода.

I. S. Rizaev, E. G. Takhavova, M. P. Shleimovich

METHODS OF IDENTIFICATION OF A HUMAN SIGNATURE*Keywords: signatures, identification, texture, classification, programming.*

The article explores methods and approaches to identify signatures of specific people. The main concepts and principles related to signature processing and analysis, including image preprocessing, feature extraction and signature classification are considered. It is indicated that a signature is a biometric feature that a person can use without the need to remember passwords or use additional devices. Various identification methods help solve the problem, for example, methods that take into account the shape, texture, and structure of the signature, speed and acceleration characterize the dynamics of signatures. In some cases, machine-learning methods are appropriate. Each of these approaches has its own advantages and limitations. There are the following signature identification methods: Template Matching, Feature Extraction and Neural Network-based Method. Their characteristics, as well as the advantages and disadvantages of these methods are given. The authors used a mathematical model to extract features: Bayesian classification, which uses probabilistic models to determine the class of an object based on its features. For software implementation, we used the Python programming language and OpenCV, an open-source computer vision library. These means help to process the signature in the following sequence: image loading; image processing; signature segmentation and image saving. A data set containing signature samples from different people provided verification the results. During the program implementation, images are pre-processed using feature extraction and classifier training based on the Bayesian approach.

Введение

Идентификация человека по подписи привлекает все больше внимания исследователей и разработчиков. Во-первых, подпись является биометрическим признаком, в этом случае могут быть использованы средства и без запоминания и хранения паролей или использования специальных дополнительных устройств. Во-вторых, подпись каждого индивидуума является уникальным представлением стиля и характера, что определяет индивидуальность каждого человека, а это является эффективным средством идентификации [1]. Идентификация человека по подписи может найти широкое применение при автоматизации документооборота, например, в банковском деле, при организации выборов, в судебных делах. Бухгалтерские отчеты можно было бы пересылать в налоговую инспекцию без личного присутствия путем отсылки документов по интернету. Для

идентификации подписей широко используются методы компьютерного зрения, что является уже областью искусственного интеллекта, которая отвечает за анализ и верность восприятия изображений [2,3]. Однако идентификация по подписи также сталкивается с рядом сложностей. Изменчивость подписей в зависимости от настроения, времени, усталости и других факторов может снижать точность идентификации. Кроме того, существует возможность подделки подписи, что делает необходимым разработку надежных методов аутентификации.

Методы и принципы исследования

В современных исследованиях и разработках в области идентификации по подписи существует несколько основных подходов и методов.

1. Методы, связанные с формой и структурой подписи:

Данный метод основан на геометрических свойствах подписей, основанных на учете точек, линий и

расстояний между ними. Также учитывается структура подписей: величина, размах, типы и величина наклонов. Скелетон и вид контура подписи может определить важные характеристики подписи [4].

2. Методы, ориентированные на вид подписей, которые характеризуются текстурными свойствами.

Этот подход основан на анализе текстурных особенностей внутри подписи. Он включает методы, такие как методы локальных бинарных шаблонов (LBP) и методы гистограмм ориентированных градиентов (HOG), которые позволяют извлекать текстурные признаки и использовать их для идентификации [5]. Текстуальные особенности подписей могут иметь самый различный вид, могут иметь волнистый вид, слоистый, рассыпчатый и т.д.

3. Методы, характеризующиеся динамическими свойствами подписей.

Данный подход рассматривает динамические свойства подписи, при которых учитывается сила давления руки и такие аспекты, как временные последовательности, а также скорость написания и даже ускорение. Примеры таких методов включают динамическое время-высотное преобразование (DTW) и скрытые Марковские модели (HMM) [6,7].

4. Методы, основанные на машинном обучении:

Данное множество представляет класс методов искусственного интеллекта. Применяется для решения задач классификации, в данном случае для идентификации подписи человека. В данном случае может быть использовано не прямое решение, а решение за счет применения обучения на примерах множества подобных задач. При решении задач классификации могут быть использованы различные алгоритмы, например, деревья решений, применение опорных векторов, случайный лес (Random Forest). При машинном обучении используются и нейронные сети. В этом случае требуется достаточно большой набор данных различных образцов подписей [7,8].

Каждый из этих подходов имеет свои преимущества и ограничения. Так, например, методы, которые в основе рассматривают форму и структуру подписей, могут быть более эффективными, так как могут быть менее требовательными в плане использования вычислительных ресурсов. Методы, основанные на динамике, в отличие от предыдущих, могут быть более устойчивыми в условиях попытки подделок подписи [9].

Для идентификации автора подписи требуется каким-то способом получить изображение подписи.

Изображение подписи можно получить различными способами. Например: 1) путем видеозаписи при ее написании, 2) путем сканирования подписи, выложенной на документе, 3) с использованием сенсорных устройств при создании цифровой подписи, 4) в некоторых случаях подписи могут формироваться с помощью различных графических устройств.

Таким образом, для создания системы идентификации подписей требуется достаточно большой объем предварительно собранных, обработанных и структурированных подписей (Dataset).

Выбор того или иного способа зависит от масштабов поставленной задачи, наличия соответствующих устройств и выставленных требований и ограничений.

После того, как подписи собраны возникает необходимость их классификации, с целью определения принадлежности подписи соответствующему человеку. При этом могут быть использованы следующие методы:

- а) путем сравнения шаблонов,
- б) путем извлечения соответствующих признаков,
- с) путем использования нейронных сетей

Преимущества и недостатки этих методов сведены в таблицу 1.

Таким образом, для идентификации подписей можно использовать сравнение с шаблоном, извлечение признаков и нейронные сети. Сравнение с шаблоном хотя и является достаточно простым и удобным методом, но при искажении подписи ведет к значительным ошибкам.

Весьма перспективным и эффективным способом является использование метода извлечения признаков. При решении задачи выделения признаков и идентификации подписей принадлежности человеку возникает задача классификации. Хотя и имеются различные методы классификации, но оказывается удобным средством является применение математической модели по Байесу. Данный метод основан на методах статистической классификации. В данном случае метод используется для определения класса объекта на основе выделенных признаков. Ниже приведена формула Байеса решения задачи классификации.

$$P(C|x) = \frac{P(x|C)P(C)}{P(x)},$$

где $P(C | x)$ - вероятность принадлежности выделенного объекта x к классу C , что соответствует апостериорной вероятности; $P(x / C)$ - вероятность наблюдения x при условии, что объект принадлежит к классу C (вероятность правдоподобия); $P(C)$ - вероятность класса C (априорная вероятность); $P(x)$ - вероятность наблюдения x .

В байесовской классификации, мы выбираем класс C , для которого апостериорная вероятность $P(C / x)$ максимальна. Для этого, мы сравниваем вероятности для каждого класса и выбираем класс с наивысшей вероятностью.

Важно отметить, байесовская классификация предполагает, что признаки независимы и имеют условно нормальное распределение. Однако, в зависимости от выбранной модели, формула может варьироваться [6]. Данный метод использует статистический подход классификации на основе теоремы Байеса. Классификация объектов (в нашем случае признаков) на основе Байесовской теоремы — это метод, который используется в статистическом машинном обучении и искусственном интеллекте для определения принадлежности объекта к определенному классу. Основная идея заключается в использовании вероятностей для оценки, насколько вероятно, что объект принадлежит к каждому из возможных классов. Ниже приведена формула Байеса:

$$P(C|X) = P(X|C) \cdot P(C) / P(X)$$

где

- $P(C|X)$ — апостериорная вероятность класса C при условии признака X .
- $P(X|C)$ — правдоподобие признака X при условии класса C .

- $P(C)$ — априорная вероятность класса C .
- $P(X)$ — нормализующая константа (вероятность признака X).

При этом:

Априорная вероятность ($P(C)$): Это вероятность того, что объект принадлежит классу до получения каких-либо данных.

Правдоподобие ($P(X|C)$): Это вероятность того, что объект имеет признак X , если он принадлежит классу C .

Нормализующая константа ($P(X)$): Это общая вероятность наблюдения признака X по всем классам. Она используется для нормализации итоговых вероятностей.

Таблица 1 - Методы идентификации подписи

Table 1 - Signature identification methods

Метод	Преимущества	Недостатки
А	Данный метод не требует большого объема предварительно собранных данных, достаточно прост при реализации	При любых искажениях подписей, изменений масштаба, наклонов, поворотов и при наличии схожих шаблонов может давать неверные результаты.
В	При извлечении признаков система может более точно классифицировать, подпис, даже при любой сложности подписей и разных стилей, при этом, система более устойчива при искажениях и масштабировании.	Система требует более сложных алгоритмов обработки. Для обучения требуется достаточно большой набор предварительно набранных данных.
С	Нейронные сети позволяют достаточно точно классифицировать подписи.. Могут обрабатывать достаточно сложные и разнообразные подписи.	Требуют большого набора обучающей выборки. Необходим подбор соответствующей архитектуры НС.

Шаги классификации заключаются в следующем:

1. Сбор данных: необходимо собрать данные с известными классами и соответствующими признаками.

2. Расчет вероятностей:

- Вычислить априорные вероятности для каждого класса.

- Вычислить правдоподобия для каждого признака, учитывая класс.

3. Применение Байесовской теоремы: Для нового объекта с известными признаками вычислить апостериорные вероятности для всех классов.

4. Классификация: Объект отнесен к классу с наибольшей апостериорной вероятностью.

При использовании байесовской классификации надо иметь ввиду, что рассматриваемые признаки независимы и условно подчиняются нормальному распределению [6].

Экспериментальная часть

Существуют различные инструменты и алгоритмы изображений. Одним из таких инструментов является

библиотека OpenCV[10]. Это библиотека компьютерного зрения с открытым исходным кодом. Данная библиотека предоставляет широкий спектр различных функций и алгоритмов для обработки изображений.

Ниже приведена последовательность обработки изображений с использованием указанной библиотеки OpenCV:

1. В начале производится загрузка изображения. При этом изображение может быть представлено в различных форматах: JPEG, PNG, BMP и других, которые поддерживаются библиотекой OpenC. Данная библиотека имеет функцию `cv2.imread()`, с помощью которой можно загрузить изображение с

подписью прямо из файла. С помощью Функции `cv2.imread()` загружает изображение и воспроизводит его в виде многомерного массива. Далее данное изображение может быть проанализировано и обработано.

2. Обработка изображения

Далее загруженное изображение подвергается обработке для улучшения качества изображения и извлечения соответствующих признаков. Нередко полученные изображения сопровождаются различными шумами. С целью отсека шумов используются различные фильтры. Для улучшения качества используются методы контрастирования.

3. Сегментация подписи

Для выделения самой подписи на фоне загруженного изображения используются алгоритмы сегментации. Сегментация позволяет отделить подпись от фона. С этой целью используют алгоритмы бинаризации. Данный алгоритм позволяет получить бинарное изображение, которое далее можно анализировать и обрабатывать.

После загрузки, обработки и сегментации подписи, полученное изображение можно сохранить для дальнейшего использования.

Для сохранения изображения в OpenCV можно использовать функцию `cv2.imwrite()`. Функция `cv2.imwrite()` сохраняет изображение в указанный файл.

Библиотека OpenCV предоставляет удобные и эффективные инструменты для получения и обработки изображений подписей.

Таким образом, используя возможности библиотеки OpenCV, мы можем реализовать этапы обработки изображения подписи для идентификации человека, который является автором этой подписи.

В дальнейшем для идентификации подписей используются алгоритмы на основе языка программирования Python и библиотеками:

- OpenCV – для обработки изображения;
- NumPy – для работы с данными.

Как ранее было отмечено, что для классификации подписей можно использовать методы на основе формы, структуры, текстуры и на основе динамических свойств. Используя одновременно все эти методы совместно можно избежать недостатки при использовании этих методов по отдельности [10,11].

Для классификации подписи воспользуемся методом извлечения признаков. В качестве статистических данных о подписи будем использовать блочное распределение пикселей на изображении. Все данные по загруженным и обработанным изображениям сохраняются в текстовом файле.

Для классификации подписей, как было изложено ранее, используют байесовский подход. Реализация алгоритма позволит определить принадлежность подписи тому или иному человеку.

С помощью библиотеки OpenCV можно извлекать и обрабатывать изображение. На приведенном ниже фрагменте показано извлечение и чтение изображения.

```
import cv2 # OpenCV
import numpy as np # NumPy
filename = input("Введите путь к изображению: ")
img = cv2.imread(filename) # Чтение изображения
cv2.imshow('Image', img)
cv2.waitKey(0)
```

Входными данными программы являются: путь к подписи, которую необходимо идентифицировать, и одновременно файл с заранее подготовленной эталонной выборкой [12,13].

В качестве обработки выделенного файла и сравнения с эталоном можно идентифицировать подпись и указать ее принадлежность конкретному человеку.

Программы идентификации начинается с подключения библиотек OpenCV. Далее вводится имя файла с исходной подписью. В результате программа отобразит исходное изображение с именем 8.jpg, представленное на рисунке 1.



Рис. 1 – Исходное изображение (8.jpg)

Fig. 1 – Original image (8.jpg)

Данная программа выделяет подпись на изображение на фоне шумов и помех, отсеивая все излишки. При этом оставляет только ту часть изображения, где имеется подпись. Данная процедура представлена на рисунке 2.



Рис. 2 – Подпись на фоне всего изображения

Fig. 2 – Signature on the background of the whole image

Полученное изображение масштабируется до величины 64x64 пикселя. После масштабирования, полученное изображение бинаризуется и выводится на экран.

Ниже приведен фрагмент программы масштабирования изображения:

```
# Масштабирование изображения до размеров 64x64
resized_image = cv2.resize(gray, (64, 64))
cv2.imshow('Resized', resized_image)
ret, binary_image = cv2.threshold(resized_image, 127, 255, cv2.THRESH_BINARY)
cv2.imshow('Binarized', binary_image)
```

Полученной бинаризованное изображение размером 64x64 делится на блоки 16x16, начиная с левого верхнего угла (рис. 3).

В итоге получается 16 блоков размером 16x16. Все изображение состоит из пустых квадратов, или отметки от частей подписи. Производится подсчет насыщения частями подписи. Пиксели, имеющие частички подписи получают 1, а пустые 0. В результате находится суммарное значение веса каждого блока. Суммарная величина веса каждого блока может изменяться от минимального равного нуля, до максимального равного 256. Таким образом, пустые блоки (см. рис 3) будут иметь вес равный нулю, а насыщенные значение, отличное от нуля.

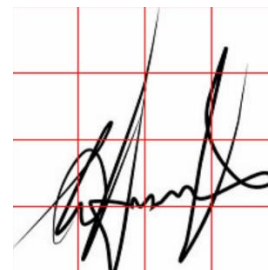


Рис. 3 – Разбиение на блоки 16x16

Fig. 3 – Breaking into 16x16 blocks

Прохождение по всему изображению и подсчет весов отображен в следующем фрагменте программы:

```
while i<64: # Прохождение по всему изображению
    j=0
```

```

while j<64:
    # Разделение на блоки
    for a in range(i,i+16):
        for b in range(j,j+16):
            # Установление значений яркости 0 или 1
            if binary_image[a,b]<10:
                binary_image[a,b] = 1
            else: binary_image[a,b] = 0
            sum = sum + binary_image[a,b] # Подсчет
# Подсчет
# весов
value = np.append(value, int(sum)) # Запись
# веса

```

На следующем этапе происходит чтение текстового файла с данными обработанной выборки.

Содержимое текстового файла представлено на рис. 4. В нем данные сгруппированы по 3 строки. Первая строка – имя владельца. Вторая строка – статистические данные о подписи. Третья строка – данные об ошибке (в этом случае используется модель, учитывающая средне квадратическое отклонение).

```

1-Jim
0.0 54.0 50.0 0.0 2.0 91.0 58.0 21.0 52.0 143.0 91.0 81.0 77.0 17.0 12.0 30.0
3.2 19.2 24.6 12.0 24.0 28.9 23.9 19.5 31.4 41.8 24.6 38.3 34.3 26.1 22.2 9.8
2-Bob
0.0 0.0 37.0 13.0 0.0 13.0 38.0 42.0 61.0 106.0 47.0 3.0 92.0 14.0 0.0 0.0
3.2 3.2 17.6 12.0 24.0 28.9 23.9 19.5 31.4 41.8 24.6 38.3 34.3 26.1 22.2 2.8
3-Adam
0.0 13.0 28.0 0.0 3.0 78.0 62.0 2.0 74.0 116.0 63.0 25.0 22.0 33.0 0.0 0.0
3.2 14.2 16.6 12.0 4.0 26.9 23.9 9.5 31.4 41.8 24.6 38.3 34.3 26.1 2.2 2.8
4-Lester
0.0 26.0 0.0 29.0 5.0 85.0 76.0 25.0 17.0 80.0 43.0 17.0 28.0 16.0 0.0 0.0
3.2 16.2 3.6 12.0 24.0 28.9 23.9 19.5 31.4 41.8 24.6 38.3 34.3 26.1 22.2 2.8
5-Andrew
0.0 15.0 77.0 0.0 67.0 118.0 62.0 0.0 127.0 139.0 63.0 99.0 107.0 15.0 63.0 2.0
3.2 16.2 24.6 12.0 24.0 28.9 23.9 19.5 31.4 41.8 24.6 38.3 34.3 26.1 22.2 4.8
6-Jack
0.0 30.0 70.0 4.0 27.0 78.0 86.0 56.0 27.0 27.0 51.0 0.0 0.0 70.0 6.0 0.0
3.2 19.2 24.6 12.0 24.0 28.9 23.9 19.5 31.4 41.8 24.6 38.3 34.3 26.1 3.2 2.8
7-Lisa
28.0 50.0 23.0 30.0 47.0 80.0 10.0 0.0 53.0 34.0 0.0 0.0 59.0 14.0 2.0 0.0
9.2 19.2 14.6 12.0 24.0 28.9 23.9 19.5 31.4 41.8 24.6 38.3 34.3 26.1 2.2 2.8
8-Anna
0.0 0.0 18.0 19.0 0.0 50.0 26.0 33.0 45.0 121.0 70.0 76.0 51.0 83.0 42.0 0.0
3.2 3.2 16.6 12.0 24.0 28.9 23.9 19.5 31.4 41.8 24.6 38.3 34.3 26.1 22.2 2.8

```

Рис. 4 – Готовые статистические данные

Fig. 4 – Prepared statistical data

На финальном шаге реализуется алгоритм байесовской классификации.

Выходным параметром является имя идентифицированного владельца подписи (строка с именем из файла). Пример:

Владелец подписи: 8-Анна

Для удобства работы число перед именем соответствует номеру распознаваемого изображения, т.е. изображения с числом 1 принадлежат Джиму, 2 – Бобу и т. д.

Точность идентификации варьируется в зависимости от того, как хорошо была подготовлена эталонная выборка. При наличии большого числа экспериментов для получения эталонной выборки точность превышает 85%. Также свою роль играет фон, на котором изображена подпись. Если после преобразования изображения программой на нем остаются фрагменты фона, то вероятность точной идентификации сильно снижается.

Результаты работы программы отображены на рисунке 5, где приведено изображение файла 6.jpg.

Программа указывает, что пользователь идентифицирован верно. Владелец подписи: 6-Jack

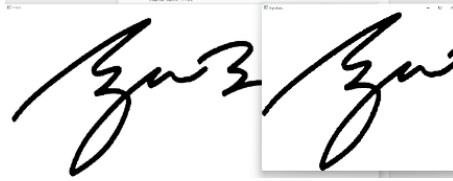


Рис. 5 – Идентификация пользователя 6

Fig. 5 – User identification 6

Надо отметить, что хорошо подготовленный эталонный образец помогает увеличить точность идентификации подписи. Проведение экспериментов показало, что при полном и хорошо подготовленном наборе образцов шаблонов можно получить точность идентификации порядка 85%

Существенную роль также играет фон, на котором изображается подпись. Если после того, как программа преобразует изображение и на нем остаются фрагменты фона, то вероятность точной идентификации значительно снижается [13,14].

Заключение

В работе были рассмотрены методы и подходы идентификации человеческих подписей. Рассмотрены основные концепции и принципы, связанные с обработкой и анализом подписей, включая предобработку изображений, извлечение признаков и классификацию подписей. Показано, что в современных исследованиях и разработках в области идентификации человека по подписи существует несколько основных подходов и различных методов. Приведены достаточно популярные методы по форме, структуре, текстуре подписи. Подписи, основанные на динамике подписи учитывают эмоциональные и физические свойства. Методы, основанные на машинном обучении, используют нейронные сети, которые хотя и дают хорошие результаты, но требуют большого набора образцов и длительное обучение. В данном случае в качестве метода идентификации и классификации воспользовался совмещенный метод, использующий характерные признаки по текстуре, форме и структуре подписи. В работе использовался набор данных, содержащий образцы подписей различных людей. В процессе реализации программы было произведено извлечение характеристик и обучение классификатора с использованием байесовского подхода [15].

Литература

1. S. Roy, M. Blumenstein, *ACM Computing Surveys (CSUR)* **49(3)**, 1-38 (2017).
2. Р. Гонсалес, *Цифровая обработка изображений*. Техносфера, Москва. 2005. 1072 с.
3. А.А. Лукьяница, *Цифровая обработка видеозаписей* Издательство «Ай Эс Эс Пресс», Москва. 2009. 518с.
4. R.Brunelli, *Template matching techniques in computer vision. Theory and practice*, Wiley, New Jersey. 2009. 339 p.
5. В. В. Трофимов, О. П. Ильина, В. И. Кияев, Е. В. Трофимова, *Информационные технологии: учебник для вузов*. Издательство Юрайт, Москва. 2023. 546 с.

6. А. Бурков, *Машинное обучение без лишних слов*. Питер, Санкт-Петербург. 2020. 192 с.
7. Е.С Петрова, *Вестник технологического университета*, **23, 5**, 825-831 (2020).
8. M.H. Siddiq, *A Review. IEEE Access*, **7**, 8890-8906 (2019).
9. М.В. Медведев, *Цифровая обработка изображений*. КНИТУ-КАИ, Казань. 2020. 100с.
10. А. Кэлер, Г. Брэдски, *Изучаем OpenCV 3*. ДМК-Пресс, Москва. 2017. 826 с.
11. I.S.Rizaev, E.G.Takhavova, *12th International Scientific and Technical Conference "Dynamics of Systems, Mechanisms and Machines"*, *Dynamics-2018* (Omsk, Russia, 2018). 2019. P. 8601417.
12. Н.А. Прохоров, В.А. Дронов, *Python3. Самое необходимое*, БХВ, Санкт-Петербург. 2019, 608 с.
13. Я.А.Фомин, *Распознавание изображений: теория и приложения*. ФАЗИС, Москва. 2010. 368с.
14. Р.М. Шакирзянов, М.П. Шлеймович, *Международный форум Kazan Digital Week – 2022*. (Казань, 20-24 сентября, 2022).
15. И.С. Ризаев, Л.М. Шарнин, З.Т. Яхина, *Перспективные информационные технологии* (Самара, 28-30 апреля, 2015). Самарский научный центра РАН. С.112-115. (2015).

References

1. S. Roy, M Blumenstein *ACM Computing Surveys (CSUR)* **49(3)**, 1-38 (2017).
2. R. Gonzalez, *Digital image processing*. Technosphere, Moscow.2005. 1072 p.

3. A.A. Lukyanitsa, *Digital processing of video images* Publishing house "ISS Press", Moscow. 2009. 518 p.
4. R.Brunelli, *Template matching techniques in computer vision. Theory and practice*, Wiley, New Jersey. 2009. 339 p.
5. V. V. Trofimov, O. P. Ilyina, V. I. Kiyaev, E. V. Trofimova, *Information technologies: textbook for universities*. Publishing house Yurait, Moscow. 2023. 546 p.
6. A. Burkov, *Machine learning without unnecessary words*. Piter, St. Petersburg. 2020. 192 p.
7. E.S. Petrova, *Herald of Technological University*, **23, 5**, 825-831 (2020).
8. M.H. Siddiq, *A Review. IEEE Access*, **7**, 8890-8906 (2019).
9. M.V. Medvedev, *Digital image processing*. KNTU-KAI, Kazan. 2020. 100 p.
10. A. Kahler, G. Bradsky, *Learning OpenCV 3*. DМК-Press, Moscow. 2017. 826 p.
11. I.S.Rizaev, E.G.Takhavova, *12th International Scientific and Technical Conference "Dynamics of Systems, Mechanisms and Machines"*, *Dynamics-2018* (Omsk, Russia, 2018). 2019. P. 8601417.
12. N.A. Prokhorov, V.A. Dronov, *Python3. The most necessary*. BHV, St. Petersburg. 2019, 608 p. 2019, 608 p.
13. Ya.A.Fomin, *Image Recognition: Theory and Applications*. FAZIS, Moscow. 2010. 368 p.
14. R.M. Shakirzyanov, M.P. Shleimovich, *International forum Kazan Digital Week – 2022* (Kazan, September 20-24, 2022).
15. I.S. Rizaev, L.M. Sharnin, Z.T. Yakhina, *Prospective information technologies* (Samara, April 28-30, 2015). Samara Scientific Center of the Russian Academy of Sciences. P.112- 115.

© **И. С. Ризаев** – к.т.н., доцент кафедры Автоматизированных систем обработки информации и управления (АСОИУ), Казанского национального исследовательского технического университета им. А.Н.Туполева (КНИТУ им. А.Н. Туполева), Казань, Россия, isr4110@mail.ru; **Э. Г. Тахавова** – к.э.н., доцент кафедры АСОИУ, КНИТУ им. А.Н. Туполева, elzzy@yandex.ru; **М. П. Шлеймович** - к.т.н., заведующий кафедрой АСОИУ, КНИТУ им. А.Н. Туполева, shlch@mail.ru.

© **I. S. Rizaev** – PhD, Associated Professor of the department of Automated Systems for Information Processing and Control (ASIPC), Kazan National Research Technical University named after A.N. Tupolev, (KNRTU named after A.N. Tupolev), Kazan, Russia, isr4110@mail.ru; **E. G. Takhavova** – PhD (Economical Sci.), Associated Professor of the ASIPC department, KNRTU named after A.N. Tupolev, email:elzzy@yandex.ru; **M. P. Shleimovich** – PhD (Technical Sci.), the Head of the ASIPC department, KNRTU named after A.N. Tupolev, shlch@mail.ru