УДК 004.032.26+004.932

Е.А. Прозорова, М.М. Немирович-Данченко

Дифференциация близнецов с использованием термограмм лица

Данная работа посвящена реализации одного из методов биометрической аутентификации, способного, с высокой долей вероятности, корректно распознать внешне идентичных людей. В рамках данной работы предпринята попытка автоматизации распознавания близнецов по их термографическим изображениям с помощью Сиамской нейронной сети. Сформулированы требования к получению термограмм с использованием тепловизора. Составлен рабочий датасет.

Ключевые слова: аутентификация, близнецы, распознавание, идентификация, биометрическая аутентификация, сиамские нейронные сети, тепловизор, термограммы, изображения.
DOI: 10.21293/1818-0442-2024-27-2-57-63

Биометрические технологии в настоящее время получают всё большее распространение, а устройства захвата (биометрические сканеры) становятся всё более совершенными. Использование биометрии основано на алгоритмах классификации, применяемых к показателям биометрических сканеров. Очень широко распространены сканеры отпечатков пальца, рукописной подписи, радужной оболочки глаза. Примером биометрии может быть и походка человека, и особенности его клавиатурного почерка. В любом случае применение методов биометрии – это процесс, в ходе которого считываются или регистрируются и анализируются анатомо-физические и поведенческие особенности человека для дальнейшей идентификации его личности [1, 2].

Это общее соображение в рамках данной работы требует уточнения. Рассматриваемая ситуация, в которой человека нужно не просто узнать, а отличить (дифференцировать) от одного или нескольких других, возможно, очень близких внешне людей.

У биометрической аутентификации есть ряд преимуществ по сравнению со стандартным способом идентификации**,** например, она может применяться бесконтактным способом. Кроме того, биометрические характеристики неотделимы от идентифицируемого пользователя, по этой же причине особо затруднены передача, подмена или искажение идентификационной информации. На сегодняшний день востребованы устройства, сканирующие физиологические характеристики человека [2]. Они используются для проведения пограничного паспортного контроля, для осуществления видеонаблюдения за объектами, а также для контроля доступа в различные учреждения [1, 3].

Как и любые другие методы аутентификации, биометрия имеет ряд минусов и уязвимостей. Биометрические данные с точки зрения злоумышленников подделать сложно, однако возможно искажение данных, предъявляемых информационной системе. Например, имеет место подделка голосовой записи (или имитации голоса с помощью нейронной сети), предъявление системе распознавания, искусственно созданный 3D-макет головы и т.д.

Тогда как подделка источника биометрической информации, т.е. человека как носителя информации, почти невозможна, имеет место использование муляжей (для аутентификации по лицу), грима, маски, слепка головы человека и т.д. [4]. Для защиты от подобной фальсификации биометрические методы следует комбинировать друг с другом и/или в сочетании с парольной защитой.

Говоря о недостатках биометрии, нужно отметить, что при взломе пароля, например, достаточной мерой может быть генерирование нового пароля, а утеря биометрических данных имеет в целом более глубокие последствия.

Биометрические методы аутентификации подразделяют на статические и динамические.

Постановка задачи

В рамках написания данной статьи ставились задачи:

– создание датасета термограмм;

– автоматизация процесса идентификации пользователей по термограммам лиц, полученным с помощью тепловизора UNI-T UTI260B;

– доказательство эмпирического предположения о том, что термограммы однояйцовых близнецов отличаются настолько, что пригодны для распознавания нейронной сетью.

Статические методы

Методы, основанные на анализе уникальных и не изменяемых со временем характеристик человека называются статическими. Данные физиологические черты считываются, например, при помощи датчиков и сравниваются с полученным заранее образцом.

К статическим методам аутентификации относится аутентификация по отпечатку пальца – дактилоскопия – это самая широко распространённая технология биометрической аутентификации.

Не менее надёжный способ – аутентификация по сетчатке глаза и радужной оболочке глаза, при этом радужная оболочка – это, как правило, менее подверженная изменениям характеристика человека, поскольку сетчатка может быть повреждена.

В аутентификации по геометрии лица или кисти рук используются физические параметры, такие как изгиб пальцев, их толщина, ширина ладони и т.д. Геометрия лица фиксируется в 3D-формате. При этом на основании 10–40 признаков отличительных элементов лица (расстояние между зрачками, высота лба, разрез глаз и т.д.) строится трёхмерная модель лица,

которая, равно как и в других методах, сравнивается с заранее полученным шаблоном.

Аутентификация по термограмме лица является одним из самых устойчивых, неизменных методов биометрической аутентификации [5]. Связано это с тем, что термограммы лиц фиксируют тепловые области, образующиеся из-за положения кровеносных сосудов, расположенных под кожей. Карта сосудов человека не меняется в процессе жизни, не зависит от процессов старения и пластических операций. Данному методу, несмотря на практические сложности с реализацией, уделяется в последнее время достаточное внимание в исследовательских работах (см., например, обзор [6]).

Динамические методы

Динамические методы аутентификации основаны на повседневных действиях – поведенческих характеристиках, которые человек демонстрирует одинаково и уникально, но в зависимости от эмоционального состояния. Фиксирование характеристик происходит во время выполнения испытуемым привычных действий, т.е. в спокойном состоянии.

Аутентификация по голосовому сигналу относится к динамическим методам. При всей технической простоте этот метод главным своим недостатком имеет изменчивость голоса – в зависимости от возраста, состояния здоровья или даже времени суток. Также критичным в данном случае является состояние окружающей среды. Внешний шум может исказить звуковую дорожку в момент записи. Кроме того, качество записи (в зависимости от устройства, с помощью которого производилась запись) также повлияет на точность и достоверность аутентификации.

К динамическим методам также относят аутентификацию по рукописному почерку, который основан на специфике написания букв и слов конкретным индивидом, а также на движении рук в момент письма. В данном случае уникальные характеристики фиксируются с помощью специальных ручек или поверхностей, чувствительных к давлению. Возможно два варианта исполнения описанного метода: анализ личной подписи и анализ динамических характеристик во время письма (времени написания, нажиме и т.д.).

Для аутентификации по клавиатурному почерку характерен анализ скорости ввода текста на клавиатуре, времени удержания и паузы между нажатиями клавиш или движения мыши. Съём информации проводится в двух вариантах: при вводе пароля или при вводе специального текста. Главным минусом данного метода является то, что клавиатурный (и рукописный) почерк может меняться в зависимости от состояния здоровья и психического состояния.

Аутентификация пользователя по термограмме лица

Аутентификация по термограмме лица – это процесс верификации заявленных пользователем данных через предъявление и регистрацию инфракрасного излучения с поверхности лица человека путём преобразования этого излучения в соответствии с заранее определённым алгоритмом в формат, обрабатываемый системой распознавания, например классификатором нейронной сети [6].

Термограмма – это изображение, чаще всего в формате BMP или PGM, демонстрирующее спектр распределения температурных полей на лице человека. Термограмма лица фиксирует тепловые узоры, появляющиеся от движения крови под кожей. Процесс создания термограммы – это, как уже было сказано выше, фиксирование градиентов температуры с помощью тепловизоров различной чувствительности.

Термограмма лица человека является одним из самых устойчивых и почти неизменных признаков, используемых в биометрической аутентификации, потому что строится на карте кровеносных сосудов, результатом сканирования которых является термограмма в SWIR-, MWIR- или LWIR-диапазонах.

В инфракрасном и ближнем инфракрасном диапазонах, NIR и SWIR спектры являются отражающими, различия во внешнем виде между видимым спектрами обусловлены свойствами отражающего материала. Таким образом, распознавание лиц оптимально производить в длинноволновом инфракрасном диапазоне в LWIR.

Большинство тепловизоров имеют разрешение 320×240 или 640×480 пикселей, что следует учитывать при снятии и дальнейшей обработке термограмм. Температурный диапазон получаемых термограмм варьируется в среднем от 26 до 36,2 °C (несмотря на то, что температура тела человека несколько выше), в зависимости от термочувствительности тепловизора [7].

Для дальнейшего успешного распознавания и идентификации человека необходимо создать несколько термограмм. Максимальное расстояние от пользователя до тепловизора, естественно, в зависимости от используемой модели и представленных характеристик, варьируется от 1 до 1,5 м. Чем ближе тепловизор к пользователю, тем выше качество получаемой термограммы.

Фон (окружающее пространство) в момент получения термограммы лица также имеет значение. Оптимальным условием для снятия термограммы будет наличие как можно большей разницей между окружающей средой и лицом человека. Внешние факторы: наличие электронного устройства, горячего предмета или постороннего человека в кадре – существенно исказят получаемое изображение. Поэтому съёмка должна производиться в помещении с температурой воздуха не более 25 °C, и чем ниже, тем лучше.

Упомянутые условия создадут разницу температур в кадре тепловизора, что критично при обработке термограмм с применением алгоритмов машинного обучения. В поле зрения нейронных сетей, производящих распознавание лица по термограмме, не должно попадать лишней информации, иначе существует вероятность получения некорректного результата [8– 10].

Критичными для качества распознавания также будут являться расположение лица на термограмме и формат получаемых изображений. Для наиболее эф-

фективного распознавания лицо человека на термограмме должно занимать центральное положение.

Применение упомянутых характеристик сопровождается рядом проблем, например отсутствием банка биометрических данных, а также высокой стоимостью программных средств, которые обеспечивают стабильность результатов и надежности идентификации.

Тем не менее, несмотря на описанные недостатки и сложности, биометрия на основе термограмм имеет некоторые преимущества перед другими методами биометрии, и эти преимущества обусловлены физиологией человека и физикой сопутствующих процессов.

Распределение температуры в организме человека далеко не случайно – это сочетание многих факторов, внутренних физиологических процессов и состояние отдельно взятых органов и тканей. В связи с этим на теле человека существуют различные области (градиенты) температуры, наличие которых связано, кроме всего прочего, с циркуляцией крови и положением сосудов под кожей.

Кровь в различных сосудах переносит тепло поразному – это сложный процесс, который практически не зависит от действий самого человека, что делает распределение температуры тела таким уникальным параметром. По этой же причине аутентификацию по термограмме осуществляет достоверное распознавание пользователей, претерпевших пластические операции. Физиологически это обосновывается тем, что хирургические вмешательства не предполагают изменения сосудистой сетки.

Исходя из всего сказанного выше, можно утверждать, что и для близнецов термограммы будут различны и уникальны.

Сигнатура лица зависит от температуры тела и подвержена искажениям со стороны естественных внешних раздражителей во время получения биометрической информации.

Идеальными условиями для создания чёткой термограммы являются помещение, температура воздуха и всех предметов мебели в котором значительно ниже температуры тела человека.

Наглядно на рис. 1 можно увидеть, что наиболее светлыми участками являются области более высокой температуры (области вокруг глаз, губ, иногда середина лба), что говорит о высокой концентрации сосудов в данных областях. Области с меньшим количеством сосудов: брови, щёки, иногда область носа (в случае наличия у субъекта гайморита) – выделены более тёмным цветом.

Важным аспектом являются способ получения термограмм пользователей и наличие на термограмме лишней информации. К лишней информации можно отнести температурную шкалу (справа), дату, время и среднюю температуру (сверху). Данный пример термограммы был получен с помощью тепловизора UNI-T UTI260B, и его не стоит использовать в процессе аутентификации, не подвергая предварительной обработке.

Рис. 1. Полученная термограмма лица без обработки

Таким образом, качество термограммы и точность дальнейшего распознавания напрямую зависят от характеристик используемого тепловизора, а также от температурного диапазона.

Аутентификация близнецов с помощью термограмм

Близнецами являются два или более потомка, рождённые от одних и тех же родителей через непродолжительное время друг за другом, внешне сложно отличимые друг от друга. Как известно, существует два типа близнецов.

Наибольший интерес в рамках данной работы представляют так называемые однояйцовые, или гомозиготные, близнецы, имеющие идентичный генотип и достаточно похожий фенотип. То есть визуально очень похожие друг на друга. Также существует и второй тип – это гетерозиготные близнецы, генетическое и визуальное сходство которых такое же, как у братьев и сестёр.

Очевидно, что наиболее сложной задачей является идентификация гомозиготных близнецов, которые всегда являются представителями одного пола и обладают портретным сходством. Отпечатки пальцев у идентичных близнецов также похожи по некоторым характеристикам (типу шаблона, количеству линий и т.д.). Известны случаи, когда гомозиготных близнецов ошибочно идентифицировала программа Face ID.

Кровеносные сосуды распределены на лице человека особенным образом, и идентичные близнецы не исключение. Термограммы двух близнецов визуально схожи ввиду одинаковой формы лица, малой разницы характерных расстояний (расстояние между глазами, высота лба и т.д.), но они в достаточной степени различны для корректного распознавания. Поэтому аутентификация близнецов с применением термограмм является наиболее эффективным методом.

В рамках данной работы были рассмотрены два индивидуума. Они являются однояйцовыми гомозиготными близнецами. Для удобства будем упоминать их как «Близнец № 1» и «Близнец № 2». Полученные и обработанные термограммы представлены на рис. 2 и 3. Термограммы были получены с одинакового расстояния, в одно и то же время, в одном и том же месте.

Согласно предварительным данным, оба близнеца обладают относительно одинаковым ростом и массой тела, также совпадают форма лица, разрез глаз и т.д. При этом полученные термограммы отличаются друг от друга. В частности, из-за разницы положения сосудов в области носа и, частично, в области щёк.

Рис. 2. Близнец № 1

Рис. 3. Близнец № 2

На рис. 2 наблюдаем более холодную область в области носа и ещё более холодную на переносице. По данным предварительного опроса студентов было выяснено, что логичное в данном случае предположение о факте перелома костей носа (или наличия заболеваний) является ошибочным и данный тепловой признак – естественный градиент температуры тела.

На рис. 3 наблюдаем более тёплую область щёк и лба по сравнению с рис. 2. Остальные области, в том числе область шеи, совпадают по температуре.

Также нужно учесть, что две термограммы получены в момент, когда близнецы находились в состоянии покоя, и данное различие термограмм нельзя списывать на разницу психоэмоциональных состояний.

Для данной работы особенно важным представляется следующее: была совершена аутентификация обоих близнецов с помощью Face ID на смартфоне одного из них. Алгоритм Face ID распознал обоих близнецов как одного и того же человека и, соответственно, снял блокировку (смартфон был разблокирован после предъявления некорректных биометрических данных).

Нейронные сети в задачах аутентификации

На сегодняшний день для решения достаточно разнообразного спектра задач, в том числе для распознавания лиц, применяются нейронные сети. Похожие алгоритмы могут быть применены в ситуации, когда требуется произвести идентификацию человека по термограмме [11].

Состоящие из нескольких слоёв и применяющие специальные алгоритмы нейронные сети проходят несколько (в некоторых случаях несколько сотен) эпох обучения для получения наилучшего результата.

Нейронные сети, алгоритмы машинного и глубокого обучения могут послужить хорошим способом автоматизации процесса идентификации человека по термограмме. А именно – выделить интересующие нас области повышенной температуры, что является сокращением времени исследования каждого изображения для идентификации конкретного индивидуума [12]. Попытка решения задачи автоматизации вышеупомянутого процесса и будет представлена в данной работе.

Следует отметить, что этот процесс может быть частично схож с процессом распознавания лиц, однако для получения более точных прогнозов и анализа градиентов температуры термограммы можно и нужно обрабатывать и преобразовывать относительно отдельной поставленной задачи с помощью некоторых математических методов.

Одним из них является использование вейвлет-преобразования Добеши [13, 14] или альтернативного ему преобразования Хаара. Использование метода KNN (метод k-ближайших соседей) также может продемонстрировать хороший результат. Суть данного алгоритма кластеризации – в определении класса объекта в зависимости от того, принадлежат ли к данному классу его ближайшие соседи, при рассмотрении в гиперпространстве признаков [15].

Создание набора данных имеет свои особенности. В нём одному индивидууму, как правило, ставится в соответствие несколько термограмм лица, сделанных в разных условиях и, возможно, с разных расстояний [16]. Часть изображений в наборе данных становится обучающей выборкой, другие – тестовой (как правило в соотношении 80% – для обучения, 20% – для тестирования). Каждое изображение обучающей и тестовой выборки кодируется в вектор признаков, затем происходит нормализация и усреднение [16, 17].

Чтобы выяснить, принадлежит ли текущее изображение тому или иному пользователю, нейронная сети в процессе классификации вычисляет Евклидово расстояние между вектором признаков тестируемого изображения и всеми остальными (в зависимости от алгоритма). В результате сравнения минимального Евклидова расстояния с заданным порогом изображению присваивается один из существующих идентификаторов. Иначе – в системе создаётся новый объект идентификации.

Точность распознавания на не предобученных моделях может достигать 30–60%, и чтобы улучшить результат, модель может достраиваться с помощью уже размеченного набора данных и с помощью увеличения количества эпох. Однако, нужно учитывать, что этот подход не сработает в тех случаях, когда, на момент создания собственного набора данных, отсутствует достаточное количество термографических изображений. Если в конкретных ситуациях исследователи вынужденно оперируют малыми объёмами термограмм, то нужно тщательно подойти к выбору модели нейронной сети, которая будет использована для аутентификации.

Сиамская нейронная сеть – это алгоритм однократного машинного обучения, который состоит из двух одинаковых сетей с идентичным набором весов. Сиамские нейронные сети применяются в условиях, например, когда стоит задача создать систему верификации личности по данным сотрудников не масштабной организации.

В подобных случаях, как правило, нет возможности получить достаточное для обучения количество фотографий каждого сотрудника, поэтому имеет смысл применения алгоритмов и моделей нейронных сетей, которые или увеличат (например, с помощью аугментации) число обрабатываемых изображений, либо будут способны корректно обрабатывать малое количество данных.

Сиамская нейронная сеть относится как раз ко второму классу моделей. Суть работы сиамской нейронной сети подразумевает создание $n + 1$ клас-

сов, где n – это изначальное количество классов сотрудников и один дополнительный класс для тех, кто сотрудниками не является.

В таком случае нейронная сеть обучается распознавать не конкретного сотрудника и присваивать ему идентификатор, а находить сходство между двумя изображениями (содержащимся в базе данных и поступающим на вход при верификации). Так происходит попарное сравнение каждого с каждым объектом классификации.

На вход Сиамской нейронной сети всегда подаются два изображения. Предполагается, что они различны (т.е. имела место попытка подмены личности при аутентификации и один человек выдаёт себя за другого). Входные данные преобразуются в векторы признаков, между которыми вычисляется разница, чаще всего для этого используют Евклидово расстояние. После сравнения значений Евклидова расстояния изображениям присваивается один и тот же класс либо два разных.

Создание набора данных

По аналогии с имеющимися в открытом доступе наборами данных термографических изображений было принято решение о создании собственного набора данных. С помощью тепловизора UNI-T UTI260B первоначально было получено 320 термограмм от двадцати разных людей (будущие 20 классов сиамской нейронной сети). Пример полученных термограмм представлен на рис. 4.

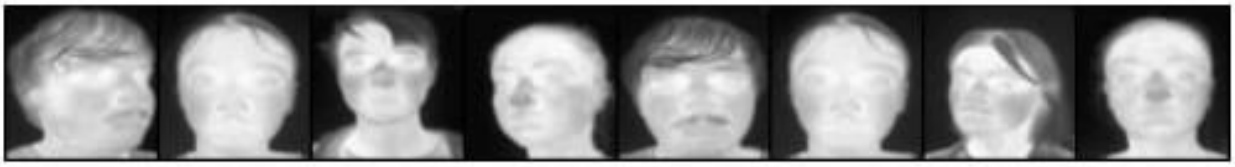

Рис. 4. Массивы термограмм для классификации

После обработки всех 320 термограмм был сформирован новый набор данных, содержащий 20 классов по 16 изображений в каждом. Размер итоговых термограмм после обработки равен 170×220 пикселей; формат итоговых изображений – PGM.

Из 20 классов два класса, учитывая особенность данной работы, были заполнены термограммами двух близнецов, уже упомянутых ранее.

Было проведено обучение на подготовленном наборе данных, который был разделён на обучающую и тестовую выборки в соотношении 80 на 20%.

В первую очередь, был создан класс, который сформирует из набора данных два массива изображений, пример одного из них – рис. 4. Элементы массивов будут сравниваться попарно.

Чем больше Евклидово расстояние, тем больше вероятность, что две термограммы принадлежат разным классам.

Например, на рис. 5 можно увидеть термограммы двух разных людей. Евклидово расстояние при этом 3,05. В среднем Евклидово расстояние, полученное при сравнении векторов признаков двух разных людей, варьируется в значениях от 0 до 10.

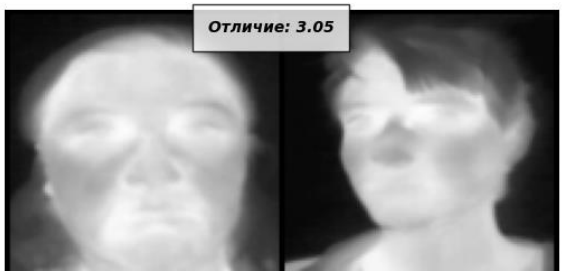

Рис. 5. Распознанные изображения

Значения Евклидова расстояния для представителей одного класса при корректном распознавании варьируются от 0 до 1.

Идентификация близнецов Сиамской нейронной сетью

Было выдвинуто предположение о следующей нулевой гипотезе: близнецы могут быть корректно распознаны на основе термограмм. Альтернативная гипотеза тогда состоит в том, что близнец № 1 может распознаваться как близнец № 2.

Была выполнена идентификация близнецов Сиамской нейронной сетью с целью доказательства эмпирического предположения о том, что термограммы однояйцовых близнецов отличаются настолько, что пригодны для распознавания нейронной сетью.

В качестве основы для идентификации был использован подготовленный набор данных. Обучающую выборку набора данных было принято решение оставить неизменной, тогда как тестовую выборку полностью составили термограммы близнецов. Результат распознавания близнецов представлен на рис. 6. В данном случае распознавание было произведено корректно.

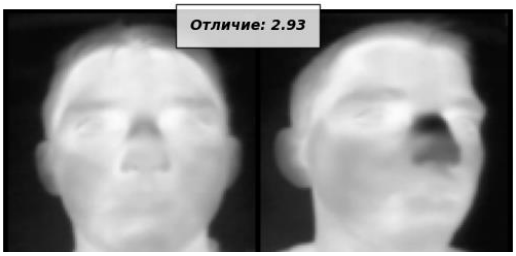

Рис. 6. Факт корректного распознавания близнецов

В процессе работы также наблюдалось некорректное распознавание близнецов. При этом полученные значения Евклидова расстояния находятся, как правило, в диапазоне 1–1,5. В то же время есть одна пара термограмм одного и того же близнеца, значение Евклидового расстояния для которой выходит из этого диапазона (точное значение 1,96) (рис. 7).

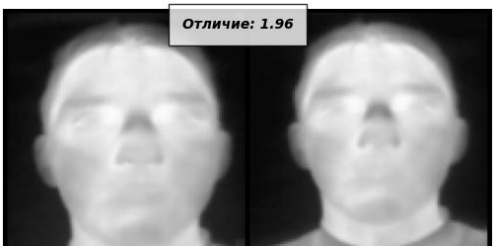

Рис. 7. Некорректное распознавание одного и того же близнеца

В результате расчётов были получены значения метрик, образующие матрицу ошибок вида Confusion Matrix (табл. 1).

Таблица 1

Матрица ошибок на основании полученных метрик

		Прогноз	
		Positive	Negative
Реальность	Positive	315	187
	Negative	38	465

Для наглядности приведем некоторые известные метрики, вычисленные с использованием матрицы ошибок: *F*-мера= 0,7368 и *recall* = 0, 8924.

При использовании архитектуры Сиамской нейронной сети наилучшие результаты показала модель, обучающаяся на описанном наборе данных, продемонстрировав наилучшее значение метрики accuracy, равное 0,7761, и значение функции потерь, равное 0,01258, при обучении на 300 эпохах. Итоговые значения точности и функции потерь в задачах идентификации обычных пользователей и близнецов представлены в табл. 2.

Таблица 2

Итоговые значения точности и функции потерь

Идентификация пользователей		Идентификация близнецов	
Accuracy	Loss	Accuracy	Loss
0,7211	0,0330	0,7761	0,0125

Заключение

В процессе выполнения работы был подготовлен собственный набор термограмм лица человека, были описаны требования по созданию такого набора данных.

На созданном наборе была проведена автоматизация процесса идентификации пользователей по термограммам лиц. В рамках выполнения работы была произведена оценка возможности идентификации близнецов Сиамской нейронной сетью. Целевой метрикой, по которой проводились оценка качества обучения и анализ результатов, являлась метрика accuracy. Значения метрик *F*-меры и *recall* демонстрируют применимость описанной методики.

Литература

1. Сабанов А.Г. Идентификация и аутентификация в цифровом мире / А.Г. Сабанов, А.А. Шелупанов. – М.: Горячая линия-Телеком, 2022. – 356 с.

2. Брагина Е.К. Современные методы биометрической аутентификации: обзор, анализ и определение перспектив развития / Е.К. Брагина, С.С. Соколов // Вестник Астраханского гос. техн. ун-та. – 2016. – Т. 2016, № 1. – С. 40–45.

3. Шаова Т.Г. Биометрические технологии – новый уровень криминалистической идентификации человека // Криминалистика – прошлое, настоящее, будущее: достижение и перспективы развития // Матер. междуна. науч.-практ. конф. – М.: Моск. академия следственного комитета Российской Федерации, 2019. – С. 639–644.

4. 3D-Face Mask Presentation Attack Detection Based on Intrinsic Image Analysis / L. Li, Z. Xia, X. Jiang, Y. Ma, F. Roli, X. Feng // IET Biom. – 2019. – P. 100–108.

5. Seal A. Human authentication based on fusion of thermal and visible face images / A. Seal, C. Panigrahy // Multimed Tools Appl. – 2019. – Vol. 78. – P. 30373–30395.

6. Mahouachi D. Recent Advances in Infrared Face Analysis and Recognition With Deep Learning / D. Mahouachi, M.A. Akhloufi // AI. – 2023. – Vol. 4. – P. 199–233.

7. Жумажанова С.С. Влияние характеристик тепловизионных систем на точность распознавания пользователя и его состояния в задачах информационной безопасности / С.С. Жумажанова, И.Д. Татаринов // Цифровизация и кибербезопасность: современная теория и практика: матер. междунар. науч.-практ. конф. – Омск: СибАДИ, 2021. – С. 228–232.

8. Обработка информации в системе идентификации по термограмме лица / М.Ю. Михеев, К.В. Гудков, Т.Н. Астахова, Е.Ю. Макарова // Вестник НГИЭИ. – 2017. – № 4 (71). – С. 7–15.

9. Thermal infrared face recognition – a biometric identification technique for robust security system / M.K. Bhowmik, K. Saha, S. Majumder, G. Majumder, A. Saha, A.N. Sarma, D. Bhattacharjee, D.K. Basu, M. Nasipur // Reviews, Refinements and New Ideas in Face Recognition. – India, Tripura University, Jadavpur University, 2011. – P. 113–138

10. Continuous 3D-Face Authentication using RGB-D Cameras / M.P. Segundo, S. Sarkar, D. Goldgof, L. Silva, O. Bellon // IEEE Conference on Computer Vision and Pattern Recognition Workshops. – USA, OR, Portland, 2013. – P. 64–69.

11. Методы выделения локальных признаков лица на изображении при аутентификации человека по термограмме / Н.И. Белов, М.А. Ермак, Е.А. Дубинич, А.Ю. Кузнецов // Научно-технический вестник информационных технологий, механики и оптики, – 2022. – Т. 22, № 2. – С. 279–286.

12. Illumination invariant face recognition using near-infrared images / S.Z. Li, R. Chu, S. Liao, L. Zhang // IEEE Trans Pattern Anal Mach Intell. – 2007. – Vol. 29, No 4. – P. 627–639.

13. A Comparative Study of Human thermal face recognition based on Haar wavelet transform (HWT) and Local Binary Pattern (LBP) / A. Seal, S. Ganguly, D. Bhattacharjee, M. Nasipuri, D.K. Basu // Computational Intelligence and Neuroscience, Department of Computer Science and Engineering. – India, Kolkata, Jadavpur University, 2013. – Vol. 2012. – 12 p.

14. Thermal imaging as a biometrics approach to facial signature authentication / A.M. Guzman, M. Goryawala, J. Wang, A. Barreto, J. Andrian, N. Rishe, M. Adjouadi // IEEE J Biomed Health Inform. – 2013. – Vol. 17, No 1. – P. 214–222.

15. Wang S. Infrared Face Recognition Based on Histogram and K-Nearest Neighbor Classification / S. Wang, Z. Liu // International symposium on neural network. – 2010. – P. 104–111.

16. Ashrafi R. A Novel Fully Annotated Thermal Infrared Face Dataset: Recorded in Various Environment Conditions and Distances from the Camera / R. Ashrafi, M. Azarbayjani, H. Tabkhi // Infrared Physics & Technology. – 2022. – Vol. 124. – P. 104209.

17. Detecting changes in facial temperature induced by a sudden auditory stimulus based on deep learning-assisted face

tracking / S. Sonkusare, D. Ahmedt-Aristizabal, M.J. Aburn, V.T. Nguyen, T. Pang, S. Frydman, S. Denman, C. Fookes, M. Breakspear, C.C. Guo // Scientific Reports. – 2019. – Vol. 9, No. 1.

Прозорова Елизавета Александровна
Магистр каф. каф. комплексной информационной безопасности электронно-вычислительных систем (КИБЭВС) Томского университета систем управления и радиоэлектроники (ТУСУР)
Ленина пр-т, 40, г. Томск, Россия, 634050
Тел.: +7-952-895-97-28
Эл. почта: el.prozorova2000@yandex.ru

Немирович-Данченко Михаил Михайлович
Д-р ф.-м. наук, профессор каф. КИБЭВС ТУСУРа
Ленина пр-т, 40, г. Томск, Россия, 634050
Тел.: +7-913-877-90-03
Эл. почта: nmm@fb.tusur.ru

Prozorova E.A., Nemirovich-Danchenko M.M.
Differentiation of twins using facial thermograms

This work is devoted to one of the little-studied methods of biometric authentication that is capable of correctly recognizing externally identical people with a high degree of probability. As part of this work, identical twins are be recognized from their thermographic images using the Siamese neural network.
Keywords: authentication, twins, recognition, identification, biometric authentication, Siamese neural networks, thermal imager, thermograms, images.
DOI: 10.21293/1818-0442-2024-27-2-57-63

References

1. Sabanov A. G., Shelupanov A. A. [Identification and authentication in the digital world]. M.: Hot Line-Telecom, 2022, 356 p. (in Russ)

2. Bragina E.K., Sokolov S.S. [Modern methods of biometric authentication: review, analysis and determination of development prospects]. *Bulletin of the Astrakhan State Technical University*, 2016, no. 1, pp. 40–45 (in Russ.).

3. Shaova T.G. [Biometric technologies - a new level of forensic identification of a person]. *Forensics – Past, Present, Future: Achievements and Development Prospects: Materials of the International Scientific and Practical Conference*, Moscow, Moscow Academy of the Investigative Committee of the Russian Federation, 2019, pp. 639–644 (in Russ.).

4. Li L., Xia Z., Jiang X., Ma Y., Roli F., Feng X. 3D-Face Mask Presentation Attack Detection Based on Intrinsic Image Analysis. *IET Biometrics*, 2019, vol. 9, no. 3, pp. 100–108.

5. Seal A., Panigrahy C. Human authentication based on fusion of thermal and visible face images. *Multimedia Tools and Applications*, 2019, vol. 78. pp. 30373–30395.

6. Mahouachi D., Akhloufi M.A. Recent Advances in Infrared Face Analysis and Recognition With Deep Learning. *AI*, 2023, vol. 4, pp. 199–233

7. Zhumazhanova S.S., Tatarinov I.D. [The influence of the characteristics of thermal imaging systems on the accuracy of recognition of the user and his state in information security tasks] *Digitalization and Cybersecurity: Modern Theory and Practice: Materials of the International Scientific and Practical Conference*. Omsk, Siberian State Automobile and Highway University (SibADI), 2021, pp. 228–232 (in Russ.).

8. Mikheev M.Yu., Gudkov K.V., Astakhova T.N., Makarova E.Yu. [Information processing in an identification system based on a facial thermogram]. *Bulletin of NGIEI (Nizhny Novgorod State Engineering and Economic University)*, 2017, no. 4(71), pp. 7–15 (in Russ.).

9. Bhowmik M.K., Saha K., Majumder S., Majumder G., Saha A., Sarma A.N., Bhattacharjee D., Basu D.K., Nasipur M. Thermal infrared face recognition – a biometric identification technique for robust security system. *Reviews, Refinements and New Ideas in Face Recognition*, India, Tripura University, Jadavpur University, 2011, pp. 113–138

10. Segundo M.P., Sarkar S., Goldgof D., Silva L., Bellon O. Continuous 3D-Face Authentication using RGB-D Cameras. *IEEE Conference on Computer Vision and Pattern Recognition Workshops.* USA, OR, Portland, 2013, pp. 64–69

11. Belov N.I., Ermak M.A., Dubinich E.A., Kuznetsov A.Yu. [Methods for identifying local facial features in an image when authenticating a person using a thermogram]. *Scientific and Technical Bulletin of Information Technologies, Mechanics and Optics*. 2022, vol. 22, no. 2, pp. 279–286.

12. Li S.Z., Chu R., Liao S., Zhang L. Illumination invariant face recognition using near-infrared images. *IEEE Transactions on Pattern Analysis and Machine Intelligence.* 2007, vol. 29, no 4, pp. 627–639.

13. Seal A., Ganguly S., Bhattacharjee D., Nasipuri M., Basu D.K. A Comparative Study of Human thermal face recognition based on Haar wavelet transform (HWT) and Local Binary Pattern (LBP). *Computational Intelligence and Neuroscience,* Department of Computer Science and Engineering, India, Kolkata, Jadavpur University. 2013, vol. 2012, 12 p.

14. Guzman A.M., Goryawala M., Wang J., Barreto A., Andrian J., Rishe N., Adjouadi M. Thermal imaging as a biometrics approach to facial signature authentication. *IEEE Journal of Biomedical and Health Informatics,* 2013, vol. 17, no. 1, pp. 214–222.

15. Wang S., Liu Z. Infrared Face Recognition Based on Histogram and K-Nearest Neighbor Classification. *International Symposium on Neural Network*, 2010, pp. 104–111.

16. Ashrafi R., Azarbayjani M., Tabkhi H. A Novel Fully Annotated Thermal Infrared Face Dataset: Recorded in Various Environment Conditions and Distances from the Camera. *Infrared Physics & Technology*, 2022, vol. 124, p. 104209.

17. Sonkusare S., Ahmedt-Aristizabal D., Aburn M.J., Nguyen V.T., Pang T., Frydman S., Denman S., Fookes C., Breakspear M., Guo C.C. Detecting changes in facial temperature induced by a sudden auditory stimulus based on deep learning-assisted face tracking. *Scientific Reports.* 2019, vol. 9, no. 1.

Elizaveta A. Prozorova
Master student, Department of Complex Information Security of Computer Systems (KIBEVS), Tomsk University of Control Systems and Radioelectronics (TUSUR)
40, Lenin pr., Tomsk, Russia, 634050
Phone.: +7-952-895-97-28
Email: el.prozorova2000@yandex.ru

Mikhail M. Nemirovich-Danchenko
Doctor of Science in Physics and Mathematics, Professor, Department of KIBEVS TUSUR
40, Lenin pr., Tomsk, Russia, 634050
Phone.: +7-913-877-90-03
Email: nmm@fb.tusur.ru