

салыстырылғанда шын мәнге ең жақыны LSTM нейрондық желісі болып табылады, ал ең нашары SARIMA моделі. Жалпы нәтижелер қанағаттандырады, себебі кез-келген акцияларды, құнды қағаздарды болжау өте қиын, өйткені экономикаға әр түрлі сыртқы факторлар әсер етеді.

Қолданылған әдебиеттер тізімі

1. Уикипедия. Временной ряд. [Электрондық ресурс]. – Электрон. дан. – Режим доступа: https://ru.wikipedia.org/wiki/Временной_ряд.
2. Уикипедия. ARIMA. [Электрондық ресурс]. – Электрон. дан. – Режим доступа: <https://ru.wikipedia.org/wiki/ARIMA>.
3. Уикипедия. Долгая краткосрочная память. [Электрондық ресурс]. – Электрон. дан. – Режим доступа: https://ru.wikipedia.org/wiki/Долгая_краткосрочная_память.
4. Proglar. Методы StandardScaler, MinMaxScaler и RobustScaler – ML. [Электрондық ресурс]. – Электрон. дан. – Режим доступа: <https://proglar.ru/blog/metody-standardscaler-minmaxscaler-i-robustscaler-ml>.

УДК 004.8

БИОМЕТРИЧЕСКАЯ ИДЕНТИФИКАЦИЯ НА ОСНОВЕ РАСПОЗНАВАНИЯ ЛИЦА

Сугуров Диас Ерланович
diassugurov@gmail.com

Магистрант 2 курса ЕНУ имени Л.Н. Гумилева, Нур-Султан, Казахстан
Научный руководитель – Бекманова Г.Т.

В статье производится анализ технологий, особенностей и преимуществ применения распознавания лица через биометрическую идентификацию. Ключевые слова: биометрическая идентификация, распознавания лица, безопасность.

Разработка биометрических приложений, таких как распознавание лиц (FR), в последнее время приобрела важное значение в умных городах. Многие ученые и инженеры по всему миру сосредоточились на создании все более надежных и точных алгоритмов и методов для таких типов систем и их приложений в повседневной жизни. FR разрабатывает технологию с несколькими приложениями в реальном времени. Целью данной статьи является разработка полной системы FR с использованием трансферного обучения в туманных вычислениях и облачных вычислениях. Разработанная система использует глубокие сверточные нейронные сети (DCNN) из-за доминирующего представления; существуют некоторые условия, включая окклюзии, выражения, освещение и позу, которые могут повлиять на производительность deep FR.

DCNN используется для извлечения соответствующих черт лица. Эти функции позволяют нам эффективно сравнивать лица между ними. Систему можно обучить распознавать набор людей и обучаться с помощью онлайн-метода, интегрируя новых людей, которых она обрабатывает, и улучшая свои прогнозы по тем, которые у нее уже есть. Предлагаемый метод распознавания был протестирован с использованием трех различных стандартных алгоритмов машинного обучения (Дерево решений (DT), К ближайших соседей (KNN), Машина опорных векторов (SVM)). Предлагаемая система была оценена с использованием трех наборов данных изображений лиц (SDUMLA-HMT, 113 и CASIA) с использованием показателей производительности точности, точности, чувствительности, специфичности и времени. Экспериментальные результаты показывают, что предложенный метод достигает превосходства над другими алгоритмами по всем параметрам. Предлагаемый алгоритм обеспечивает более высокую точность (99,06%), более высокую точность (99,12%), более высокую отзывчивость (99,07%) и более высокую специфичность (99,10%), чем алгоритмы сравнения.

Кроме того, система FR обеспечивает огромные преимущества по сравнению с другими решениями биометрической безопасности, такими как отпечатки ладоней и отпечатки пальцев. Система фиксирует биометрические измерения человека с определенного расстояния, не взаимодействуя с человеком. В приложениях для сдерживания преступности эта система может помочь многим организациям идентифицировать человека, у которого есть какое-либо уголовное прошлое или другие юридические проблемы. Таким образом, эта технология становится незаменимой для многочисленных жилых зданий и корпоративных организаций.

Этот метод основан на способности распознавать человеческое лицо, а затем сравнивать различные черты лица с ранее записанными лицами. Эта функция также повышает важность системы и позволяет широко использовать ее по всему миру. Он разработан с удобными для пользователя функциями и операциями, которые включают в себя различные узловые точки лица. Существует примерно от 80 до 90 уникальных узловых точек лица. Из этих узловых точек система FR измеряет важные аспекты, включая расстояние между глазами, длину линии подбородка, форму скул и глубину глаз. Эти точки измеряются путем создания кода, называемого *faceprint*, который представляет идентификацию лица в компьютерной базе данных. С внедрением новейших технологий системы, основанные на 2D-графике, теперь доступны на 3D-графике, что делает систему более точной и повышает ее надежность.

Биометрия определяется как наука и технология для измерения и статистического анализа биологических данных. Они представляют собой измеримые поведенческие и/или физиологические характеристики, которые могут быть использованы для проверки индивидуальной идентификации. Для каждого человека для проверки можно было бы использовать уникальную биометрическую информацию. Биометрические системы используются во все большем количестве областей, таких как безопасность тюрем, защищенный доступ и судебно-медицинская экспертиза. Биометрические системы распознают людей с помощью аутентификации, используя различные биологические особенности, такие как лицо, геометрия руки, радужная оболочка, сетчатка и отпечатки пальцев.

Система FR - это более естественный процесс получения биометрической информации с лучшими вариациями, чем любой другой метод. Таким образом, FR стала недавней темой в информатике, связанной с биометрией и машинным обучением.

Машинное обучение - это область компьютерных наук, которая дает компьютерам возможность учиться без дальнейшего явного программирования. Основным направлением машинного обучения является предоставление алгоритмов для обучения выполнению задачи — машинного обучения, относящегося к области вычислительной статистики и математической оптимизации. Машинное обучение включает в себя множество методов, таких как обучение с подкреплением, контролируемое обучение, почти контролируемое обучение и обучение без присмотра.

Машинное обучение может быть использовано для многих задач, которые, по мнению людей, могут выполнять только они, таких как игры, изучение предметов и распознавание. Большинство алгоритмов машинного обучения потребляют огромное количество ресурсов, поэтому было бы лучше выполнять их задачи в распределенной среде, такой как облачные вычисления, туманные вычисления или пограничные вычисления. Чтобы обучить нейросети, используют огромные базы данных с лицами людей. Нейросети на входе сообщают, кому принадлежит это лицо, а затем, в ходе обучения, добиваются, чтобы она выдавала максимально точные результаты. Обучившись на миллионах разных людей, нейросеть начинает распознавать и новые лица — те, которых не было в базе[2].

Анализ мирового потока научных работ по данному направлению методами наукометрических исследований позволяет увидеть объективную картину развития данного научного направления и оценить его актуальность и потенциальные возможности

применения. Повышение надежности систем аутентификации личности является актуальной научно-технической задачей[3].

Это более естественный процесс получения биометрической информации, чем другие предлагаемые системы, и он должен учитывать больше вариаций, чем любой другой метод. Это одна из самых известных задач комбинаторной оптимизации. Решение этой проблемы в разумные сроки требует эффективного метода оптимизации. FR может столкнуться со многими трудностями и проблемами с точки зрения входного изображения, такими как различное выражение лица, объекты в шляпах или очках и различные уровни яркости. Это исследование основано на адаптивной версии самого последнего алгоритма DCNN, называемого AlexNet. В этой статье предложен метод глубокого обучения FR с использованием TL в вычислениях fog. Предлагаемый алгоритм DCNN основан на наборе шагов для обработки изображений лица для получения отличительных черт лица. Эти этапы разделены на предварительную обработку, распознавание лиц и извлечение объектов. Предлагаемый способ улучшает решение за счет настройки параметров для поиска окончательного оптимального решения. В этом исследовании предлагаемый алгоритм и другие популярные алгоритмы машинного обучения, включая алгоритмы DT, KNN и SVM, были протестированы на трех стандартных контрольных наборах данных, чтобы продемонстрировать эффективность и действенность предлагаемого DCNN в решении проблемы FR. Эти наборы данных характеризовались различным количеством изображений, включая мужчин и женщин. Предложенный алгоритм и другие алгоритмы были протестированы на различных изображениях в первом наборе данных, и результаты продемонстрировали эффективность алгоритма DCNN с точки зрения достижения оптимального решения (т.е. наилучшей точности) с разумной точностью, отзывом, точностью и специфичностью по сравнению с другими алгоритмами. В то же время предложенный DCNN достиг наилучшей точности по сравнению с Jonnathann et al. Точность предложенного метода достигла 99,4% по сравнению с 97,26% у Джоннатанна и др. Предлагаемый алгоритм обеспечивает более высокую точность (99,06%), более высокую точность (99,12%), более высокую отзывчивость (99,07%) и более высокую специфичность (99,10%), чем алгоритмы сравнения[4].

Какие же преимуществами обладает данный способ идентификации?

1) Повышение безопасности.

На государственном уровне распознавание лиц может помочь идентифицировать террористов или других преступников. На личном уровне распознавание лиц можно использовать как инструмент безопасности для блокировки устройств и в личных камерах видеонаблюдения.

2) Снижение уровня преступности.

Распознавание лиц упрощает поиск грабителей, воров и правонарушителей. Одно только знание о присутствии системы распознавания лиц может служить сдерживающим фактором, особенно в отношении мелких преступлений. Помимо физической безопасности, имеются преимущества и в сфере кибербезопасности. Компании могут использовать технологию распознавания лиц вместо паролей для доступа к компьютерам. Теоретически эту технологию невозможно взломать, поскольку красть или менять, как в случае с паролем, нечего.

3) Устранение предвзятости при остановке и обысках.

Обеспокоенность общественности по поводу необоснованных остановок и обысков является источником разногласий в полиции. Технология распознавания лиц может улучшить этот процесс. Выявление подозрительных личностей в толпе с помощью автоматизированного, а не управляемого человеком процесса, такого как технология распознавания лиц, может снизить потенциальную предвзятость и сократить количество остановок и обысков законопослушных граждан.

4) Удобство.

По мере распространения технологии распознавания лиц, покупатели смогут расплачиваться в магазинах, используя собственное лицо, и не вынимать кредитные карты или наличные деньги. Это позволит сэкономить время в очереди к кассе. Поскольку для распознавания лиц не требуется никакого контакта, как при снятии отпечатков пальцев или выполнении других мер безопасности, эта технология особенно полезна во время эпидемии COVID. Распознавание лиц обеспечивает быструю, автоматическую и беспроblemную проверку.

5) Быстрая обработка.

Процесс распознавания лица занимает всего секунду, что дает преимущества компаниям, использующим технологию распознавания лиц. В эпоху кибератак и продвинутых инструментов взлома компаниям нужны безопасные быстрые технологии. Распознавание лиц позволяет быстро и эффективно проверить личность человека.

6) Интеграция с другими технологиями.

Большинство решений для распознавания лиц совместимы с программами обеспечения безопасности. Фактически, эта технология легко интегрируется. Это снижает объем дополнительных инвестиций, необходимых для ее внедрения[5].

В заключении, нужно отметить, что технология распознавания лиц стремительно развивается и применяется уже в повседневной жизни человека и существенно облегчает некоторые процессы, такие как открытие банковской карты онлайн через смартфон или же авторизация на портале государственных услуг и получение ЭЦП, всё это происходит онлайн и только благодаря распознаванию лиц. В ходе данной статьи была проанализирована технология биометрической идентификации через лицо и её основные преимущества. В рамках диссертационной работы будет представлено мобильное приложение, в ходе использования которого можно ознакомиться с проведенным исследованием и функционалом.

Список использованных источников

1. Друки А. А. Система поиска, выделения и распознавания лиц на изображениях // Известия Томского политехнического университета [Известия ТПУ]. — 2011. — Т. 318, № 5. — С. 64—70.
2. Гэри Маркус, Эрнест Дэвис. Искусственный интеллект: Перезагрузка. Как создать машинный разум, которому действительно можно доверять = Rebooting AI: Building Artificial Intelligence We Can Trust. — М.: Интеллектуальная Литература, 2021. — 304 с.
3. Nilsson, Nils J. (2009). The Quest for Artificial Intelligence. Cambridge University Press
4. R. Brunelli and T. Poggio, "Face Recognition: Features versus Templates", IEEE Trans. on PAMI, 1993
5. Crawford, Mark. "Facial recognition progress report". SPIE Newsroom. Retrieved October 6, 2011.

ӘОЖ 004.75

ЖЕЛІЛІК ҚАУІПСІЗДІКТІ JUNOS ОЖ НЕГІЗІНДЕ БАСҚАРУ

Тоқтыбаев Иса Асхатұлы

isa.toktybaev@gmail.com

Л.Н.Гумилев атындағы ЕҰУ Ақпараттық технологиялар факультетінің ақпараттық қауіпсіздік кафедрасының магистранты, Нұр-Сұлтан, Қазақстан
Ғылыми жетекші – аға оқытушы, PhD Ж.М. Ташенова

Қазіргі заманғы күрделі желілік архитектурада және үнемі өзгеріп отыратын ортада IT мамандарына қауіпсіздікті тиімді деңгейде сақтау қиынға соғады. Қауіпсіздікті қамтамасыз ету жөніндегі әкімшілік міндеттерге пайдаланушылардың, құрылғылардың, орналасу