



СПбГЭТУ «ЛЭТИ»
ПЕРВЫЙ ЭЛЕКТРОТЕХНИЧЕСКИЙ



А.Е. Сулавко

Машинное обучение в приложениях биометрии

**Нейросетевой подход к анализу и
классификации биометрических
образов**

Конспект лекции

СПбГЭТУ «ЛЭТИ», 2022 г.





НЕЙРОСЕТЕВОЙ ПОДХОД К АНАЛИЗУ И КЛАССИФИКАЦИИ БИОМЕТРИЧЕСКИХ ОБРАЗОВ

Особое место среди методов машинного обучения, совершенно точно, занимают искусственные нейронные сети (ИНС), представляющие собой математическую модель, а также ее программные или аппаратные реализации, построенную в некотором смысле по образу и подобию сетей нервных клеток живого организма. Свое широкое распространение ИНС получили относительно недавно, несмотря на то, что первые попытки их исполнения были предприняты еще в середине прошлого века. Во многом «возрождение» нейронных сетей и их повсеместное применение сегодня обусловлено прорывным событием середины 2000-х годов, когда группы исследователей из университета Торонто (под руководством Джеффри Хинтона) и университета Монреаля (под руководством Йошуа Бенджи) научились обучать глубокие нейронные сети. Стоит отметить также, что идеи самого по себе глубокого обучения также не являлись новыми для мира машинного обучения, однако не были реализованы ранее во многом в виду нехватки вычислительных ресурсов компьютеров второй половины XX века (что уже не являлось проблемой в 2005 г.). Глубокие искусственные нейронные сети (глубокие ИНС) на сегодняшний день уже не являются чем-то сверхъестественным и, как было отмечено выше, получили повсеместное распространение в самых разных областях человеческой деятельности.

Говоря об архитектуре глубоких ИНС, стоит отметить, что они представляют собой сложную структуру, состоящую из большого количества внутренних (скрытых) слоев с настраиваемыми параметрами — весовыми коэффициентами искусственных нейронов, составляющих каждый слой сети. На первый, входной слой сеть принимает вектор признаков, описывающих объект — данные в виде сигналов. На внутренних слоях происходит их обработка: входной вектор умножается на матрицу связей, и сформированный таким образом вектор новых признаков передается в следующий слой. Результат обработки сигнала отправляется на выходной слой сети.

Каждая нейросеть содержит множество параметров, которые невозможно настроить вручную, и поэтому обучают ГНС на массиве данных: в





процессе обучения и переобучения весовые коэффициенты нейронов непрерывно меняются и настраиваются так, что результат вычислений и обработки сигналов становится осмысленным. Настройка весовых коэффициентов производится методом обратного распространения ошибки, построенном на пакетной или стохастической реализации градиентного спуска[8].

На больших объемах данных глубокое обучение показывает более высокую точность результатов в сравнении с традиционным машинным обучением. Однако недостатками ГНС является сложность интерпретации получаемых результатов, невозможность автоматического обучения подобных сетей, а также их склонность к переобучению.

Во многом, перечисленных выше недостатков глубоких ИНС позволяют избежать так называемые «широкие» ИНС. Важной характеристикой таких сетей является процедура автоматического обучения (без использования градиентного спуска). Обучение выполняется послойно, каждый нейрон обучается независимо от остальных нейронов сети, исходя из параметров закона распределения признаков, вычисляемых по данным обучающей выборки. Добавление нейронов, увеличение числа входов и выходов сети не приводит к росту объемов обучающей выборки, а ведет к снижению количества ошибок (до определенного предела). Для обучения «широких» нейронных сетей, как правило, требуется значительно меньший объем выборки, чем для обучения многослойных нейронных сетей.

Помимо классических ИНС, все большее распространение получают сверточные нейронные сети (CNN), впервые предложенные Яном Лекуном в 1988 году и не являющиеся явным развитием идеи ограниченных машин Больцмана и подхода Хинтона. Сверточные сети существенно сокращают сложность нейросетевой обработки, так как снижают размерность задачи.

В нейронной сети подобного типа применяются последовательная комбинация из трех типов слоев. Первый тип - свертка - извлекает информативные признаки, имеющие структурную организацию. Второй тип - субдескритизация - благодаря пространственному сжатию данных обеспечивает инвариантность отклика слоя к малому смещению паттерна. Третий тип - многослойный персептрон. Первые два типа слоев (convolutional, subsampling), чередуясь между собой, формируют входной вектор признаков





для многослойного персептрона. Ключевой операцией для сверточных ИНС является операция свертки. Сверточные сети отличаются очень высокой способностью к распознаванию паттернов на изображениях, поэтому теоретически применимы к задачам распознавания и классификации, в том числе, биометрических образов, однако такой тип сетей оказывается неустойчив к состязательным атакам в виде шумов, накладываемых на распознаваемое изображение. В частности, при использовании сверточных ИНС в биометрических приложениях, значительно увеличивается FAR.

Еще одной архитектурой ИНС, заслуживающей внимания в вопросах работы, в том числе, с биометрическими образами, являются автокодировщики. Особенно хорошо такой вид ИНС зарекомендовал себя в задачах снижения размерности, частным случаем которых является задача извлечения признаков. Автокодировщик состоит из двух компонентов, кодировщика и декодировщика, каждый из которых может иметь одинаковое количество скрытых слоев. Кодировщик учится сжимать входной вектор X до более короткого кода h , в то время как декодировщик учится восстанавливать входной вектор X , распаковывая h [13].

Основной принцип работы и обучения сети автокодировщика — получить на выходном слое отклик, наиболее близкий к входному. Чтобы решение не оказалось тривиальным, на промежуточный слой автокодировщика накладывают ограничения: промежуточный слой должен быть или меньшей размерности, чем входной и выходной слои, или искусственно ограничивается количество одновременно активных нейронов промежуточного слоя — разреженная активация. Эти ограничения заставляют нейросеть искать обобщения и корреляцию в поступающих на вход данных, выполнять их сжатие. Таким образом, нейросеть автоматически обучается выделять из входных данных общие признаки, которые кодируются в значениях весов искусственной нейронной сети. Так, при обучении сети на наборе различных входных изображений, нейросеть может самостоятельно обучиться распознавать линии и полосы под различными углами.

Чаще всего автокодировщики применяют каскадно для обучения глубоких (многослойных) сетей. Автокодировщики применяют для предварительного обучения глубокой сети без учителя. Для этого слои обучаются друг за другом, начиная с первых. К каждому новому необученному





слою на время обучения подключается дополнительный выходной слой, дополняющий сеть до архитектуры автокодировщика, после чего на вход сети подается набор данных для обучения. Веса необученного слоя и дополнительного слоя автокодировщика обучаются при помощи метода обратного распространения ошибки. Затем слой автокодировщика отключается и создается новый, соответствующий следующему необученному слою сети. На вход сети снова подается тот же набор данных, обученные первые слои сети остаются без изменений и работают в качестве входных для очередного обучаемого автокодировщика слоя. Так обучение продолжается для всех слоев сети за исключением последних. Последние слои сети обычно обучаются без использования автокодировщика при помощи того же метода обратного распространения ошибки и на маркированных данных (обучение с учителем).

Все рассмотренные выше архитектуры ИНС так или иначе используются в задачах анализа биометрических образов.

Работа с данными. Как и при реализации статистического подхода к анализу и классификации биометрических образов, при работе с ИНС данные, поступающие на вход той или иной модели, необходимо предварительно обрабатывать: нормализовывать, очищать (например, от шумов), разделять на тестовую и обучающую выборки, а также выполнять ряд других операций целью повышения качества имеющихся данных. Все перечисленные методы обработки данных позволяют повысить эффективность работы модели, а также избежать некорректного процесса обучения.

Помимо обработки уже имеющихся данных, может возникнуть потребность в создании дополнительных. В машинном обучении такую операцию принято называть аугментацией данных. Наиболее актуальной данная методика является для глубоких нейронных сетей, так как для их обучения требуются большие объемы обучающих выборок.

Все преобразования, используемые в аугментации, можно выделить в две категории. Первые опираются на информацию о процессе обучения модели и ее свойства. Вторые используют априорные знания о данных для конкретной задачи.





В случае работы с изображениями, типы аугментации соответствуют следующим группам: яркостные, геометрические, зашумления, аддитивные (наложение двух изображений). Выбор преобразований обычно происходит на основе возможных деформаций на изображениях. Так, в задаче распознавания символов, снятых на цифровую камеру, наиболее актуальны сглаживание, проективные искажения, яркостные изменения, добавление гауссового шума, повороты. При распознавании симметричных объектов можно использовать отражения по какой-либо оси.

Помимо выше упомянутых “классических” видов преобразований в последнее время предпринимаются попытки использовать для аугментации генеративно-сопоставительные сети (generative adversarial networks, GANs)

Производить генерацию дополнительных комбинаций данных, используя уже имеющиеся, исторические, данные можно также по средствам метода Монте-Карло. В общем случае, методы Монте-Карло представляют собой подмножество вычислительных алгоритмов, которые используют процесс многократной случайной выборки для численных оценок неизвестных параметров. Использование методов Монте-Карло невероятно широко и привело к ряду принципиально новых открытий в самых разных областях человеческой деятельности[14].

Все перечисленные выше методы можно отнести к инструментам генерации синтетических данных, то есть данных, генерируемых в случае, когда реальные данные отсутствуют или их сбор невозможен (из-за большой длительности или дороговизны процесса). Чаще всего наборы данных генерируются полностью случайным образом на основе некой статистической модели, которая учитывает законы распределения реальных данных. Использование корректно сгенерированных синтетических данных (качество сгенерированных данных должно соответствовать качеству реальных данных, также важны детализации и семантика объектов в данных — они должны соответствовать реальным) может улучшить качество работы нейронных сетей и различных алгоритмов машинного обучения. Синтетические данные также позволяют привнести в датасет те объекты, которые редко встречаются в реальных данных или те, которые еще не были зафиксированы в реальных данных, но ясно как их сконструировать.





Нейросетевые преобразователи биометрия-код (НПБК). В отечественной практике в основе нейросетевого подхода к анализу и классификации биометрических образов лежит концепция нейросетевого преобразователя биометрия-код (НПБК), подробного описанного и рассмотренного в серии стандартов ГОСТ Р 52633, разработанных в Пензенском научно-исследовательском электротехническом институте под руководством доктора технических наук Иванова Александра Ивановича[15].

Согласно первому (из указанной выше серии стандартов) стандарту ГОСТ Р 52633.0-2006, нейросетевой преобразователь "биометрия-код" - это заранее обученная искусственная нейронная сеть с большим числом входов и выходов, преобразующая частично случайный вектор входных биометрических параметров "Свой" в однозначный код криптографического ключа (длинного пароля) и преобразующая любой иной случайный вектор входных данных в случайный выходной код. НПБК позволяет не просто осуществлять биометрическую идентификацию/верификацию пользователя, но и выполнять ее таким образом, чтобы данные пользователя не оказались скомпрометированы. В сущности, вся концепция ПБК позволяет перейти от простой биометрической идентификации/верификации к биометрико-криптографической идентификации/верификации, связывающей криптографические и биометрические методы с целью «привязки» высоконадежного криптографического ключа к биометрическим образам человека.

При построении нейросетевой ПБК формируется ИНС, количество входов которой равно числу признаков, а количество выходов - длине его личного ключа. Каждый нейрон последнего слоя генерирует один или более бит. Нейронная сеть обучается на биометрических образах пользователя и образах «Чужих», чтобы вырабатывать ключ субъекта при отступлении на вход его биометрического образа. Обучение нейросетевого ПБК должно быть автоматическим, при этом объем обучающей выборки «Чужие» может быть сколь угодно большим. Важно, что число примеров «Свой» для обучения нейросетевого ПБК должно быть малым (не менее 11), так как нельзя заставить пользователя предоставлять свой образ многократно. Это обстоятельство накладывает ограничение на ИНС, используемую в основе





ПБК. Именно поэтому для построения нейросетевых ПБК используются неглубокие архитектуры (shallow networks), а именно «широкие» сети.

Так как НПБК должен откликаться на примеры образа «Свой» одним кодом ($\bar{c}$), а на другие образы «Чужой» - случайными кодами ($\bar{z}_i$), то код «Свой» и случайные коды образов «Чужие» не совпадают между собой по состояниям части разрядов. В качестве меры близости кодов образов «Чужие» к коду «Свой» можно использовать расстояние Хэмминга h_i . Расстояние Хэмминга вычисляется сложением по модулю два разрядов с одинаковыми номерами k сравнимых кодов длиной n с последующим подсчетом выявленных состояний «1» обычным суммированием

$$h_i = \sum_{k=1}^n (c_k \oplus z_{k,i})$$

При полном совпадении разрядов сравниваемых кодов $h_i = 0$, а при полном несовпадении их $h_i = n$, т.е. число дискретных величин h_i принимает $n+1$ состояние. Если теперь подавать случайные образы «Чужой» на вход обученного преобразователя «биометрия-код», то сформируется серия кодов откликов $\bar{z}_i$, которая будет характеризоваться некоторым распределением расстояний Хэмминга h_i [16].

Стоит отметить, что «широкие» нейронные сети, лежащие в основе НПБК, имеют определённые ограничения:

Сниженная длина ключа (достаточная не для всех биометрических модальностей);

Возможность проведения атаки «извлечения знаний» из обученного нейросетевого ПБК путем статического анализа стабильности выходов ПБК при поступлении на его входы естественных и синтетических образов «Чужих» (существуют методы предотвращения подобного эффекта) [7]

Конечно, решение задач распознавания биометрических образов не ограничивается применением «широких» сетей. Для подобных задач теоретически могут использоваться и иные архитектуры НС, рассмотренные выше, такие, как глубокие нейронные сети, сверточные нейронные сети (в том числе многослойные), автокодировщики и т.д.





Однако для построения НПБК затруднительно использовать многослойные сетевые архитектуры, особенно персептроны, обучаемые по принципу обратного распространения ошибки и имеющие обычно один выход (при классификации двух образов - «Свой» и «Чужой»). Дело в том, что формирование и обучение ПК в биометрии, должно быть автоматическим, но практически все итерационные алгоритмы имеют существенную склонность к переобучению. Свёрточные нейронные сети, в целом, дают более показательные результаты, но при анализе слабых биометрических образов вероятности ошибок оказываются значительными (особенно для голосовых образов). Дело в том, что итерационные алгоритмы настройки весов нейронов неустойчивы на малых обучающих выборках (методы оптимизации сети не делают алгоритм обучения абсолютно устойчивым, что требуется в биометрии).

Чем выше информативность биометрического образа (т.е. уникальность и стабильность признаков), тем меньший объём выборки нужен и тем более стабильной оказывается итерационная процедура обучения. Например, для настройки свёрточных нейронных сетей в задаче биометрической идентификации личности по лицу достаточно пяти примеров изображения лица от каждого идентифицируемого субъекта (в различных ракурсах). Однако образ лица гораздо информативней, чем голосовой или рукописный образ. Поэтому при распознавании диктора или подписи процедуры итерационного обучения менее стабильны.

Одним из возможных подходов к применению глубоких нейронных сетей в задачах построения НПБК является подход, заключающийся в комплексировании глубоких и широких сетей (помимо комплексирования глубоких НС и нечетких экстракторов). В таком случае глубокие нейронные сети используются в качестве экстракторов признаков из биометрических образов. Извлечение признаков с помощью многослойных нейронных сетей нельзя приравнивать к генерации ключа на основе биометрических данных, так как к криптографическим ключам и паролям предъявляются определенные требования, связанные с их длиной и энтропией. Признаки, непосредственно извлеченные из биометрического образа, не обладают соответствующими свойствами. Извлечение признаков - это лишь этап обработки образа в системе связывания предварительно сгенерированного





ключа и биометрических параметров субъекта. Поэтому для корректного построения НПБК такой экстрактор следует связывать с классическим НПБК на основе «широкой» сети.

Доверие к средствам высоконадежной биометрической аутентификации определяется результатами их тестирования, выраженными в форме гарантий производителя, подтвержденных, по необходимости, сертификационными документами. Тестирование средств биометрической аутентификации проводится с использованием баз биометрических образов "Свой" и "Чужой", размеры которых являются достаточными для подтверждения характеристик тестируемых средств. Наиболее сложной частью задачи является тестирование стойкости обученных преобразователей "биометрия-код" к атакам подбора. Такое тестирование производится согласно ГОСТ Р 52633.3. согласно данному стандарту стойкость к атакам подбора - это показатель, определяющий число попыток подбора, необходимое злоумышленнику для получения на выходе преобразователя неизвестного ему кода доступа "Свой" при использовании для атаки заранее сформированной базы биометрических образов "Чужой".

Как правило, создать достаточно большой объем естественных биометрических образов технически невозможно. По этой причине приходится многократно увеличивать размеры тестовой базы биометрических образов за счет синтетических биометрических образов, созданных по ГОСТ Р 52633.2.

