Верификация на котах

En Verification on Cats

V. A. Konyavskiy,
PhD (Eng., Grand Doctor)
konyavskiy@gmail.com

S. A. Trenin
s.trenin@gmail.com

Moscow Institute of Physics and Technology

I. A. Abdullaeva
a.irene.a@mail.ru

Bauman Moscow State Technical University

It is impossible to provide secure access to remote services in the digital economy using untrustworthy client devices (smartphones) without building a verification model that is resistant to spoofing, copying, or imitating data that identifies a person. This article discusses a procedure that takes into account characteristics of a person's reflex reactions in the process of identity confirmation. An example of a corresponding verification model is described, a method for its construction, and also the quality estimates obtained in experiments are given. The proposed model is based on a neural network, and the decision on identity verification is made based on the analysis of information about a person's reactions to visual stimuli. The achieved quality turns out to be quite high (comparable to known analogs), while the requirements for sensors in experiments are significantly reduced.

Keywords: biometry, interactive biometry, interactive reflex biometry, identification, verification, eye movement verification, interactive reflex identification, digital identification, identification in a digital society

Обеспечить безопасный доступ к удаленным сервисам цифровой экономики при использовании недоверенных клиентских устройств (смартфонов) невозможно без построения модели верификации, устойчивой к подмене, копированию или имитации данных, идентифицирующих человека. В настоящей статье рассматривается процедура, учитывающая особенности рефлекторных реакций человека в процессе подтверждения личности. Описан пример соответствующей модели верификации, способ ее построения, а также приведены оценки качества, полученные в ходе экспериментов. В основе предложенной модели лежит нейронная сеть, а решение о верификации личности принимается на основе анализа информации о реакциях человека на визуальные стимулы. Достигнутое качество оказывается достаточно высоким (сравнимым с известными аналогами), в то время как требования к сенсорам в экспериментах существенно сокращены.

Ключевые слова: биометрия, интерактивная биометрия, интерактивная рефлекторная биометрия, идентификация, верификация, верификация по движению глаз, интерактивная рефлекторная идентификация, цифровая идентификация, идентификация в цифровом обществе

Валерий Аркадьевич Конявский,
доктор технических наук, ведущий научный сотрудник
konyavskiy@gmail.com

Сергей Алексеевич Тренин
s.trenin@gmail.com

Московский физико-технический институт

Ирина Альбертовна Абдуллаева
a.irene.a@mail.ru

Московский государственный технический университет им. Н. Э. Баумана

Настоящая статья продолжает цикл публикаций о ходе исследовательских работ по направлению интерактивной рефлекторной биометрии, основные идеи которых заложены в [1]. В [2] рассматривалась необходимость и целесообразность применения этих методов в информационных системах цифровой экономики. Общие принципы работы со стимулами и реакциями на них, а также схема работы системы интерактивной идентификации, устойчивой к подмене идентификатора, сформулированы и подробно прокомментированы в [3], а инструментальный комплекс для этого – в [4]. В этой же статье описывается схема предложенной нами методики верификации с использованием данных о парах «стимул – реакция».

Мы представляем результаты исследования, целью которого было экспериментальное подтверждение гипотезы о существовании приемлемой модели верификации.

Если некоторая модель верификации демонстрирует высокое качество, то этот факт является серьезным аргументом в пользу исследуемой гипотезы. Кратко охарактеризуем основные особенности собранного набора данных и использованных для его подготовки стимулов, а также приведем разработанную нами общую схему моделей верифи-

кации, среди которых нам удалось обнаружить именно ту, которая показывает хорошие результаты. В завершение кратко опишем использованную методику оценки качества и приведем численные значения полученных в ходе экспериментов оценок качества.

Исследуемый вид стимулов и индуцируемых реакций

В качестве стимула мы рассматриваем точку, перемещающуюся по непрерывной траектории. Непрерывное и плавное перемещение точки по экрану приводит к регистрации доминирующего числа следящих движений, длительность и непрерывность которых зависит от скорости перемещения стимула и объясняется физиологическими возможностями глаза человека [5–7].

Для подобных движений, в свою очередь, оказывается характерной как существенная зависимость от стимула, так и относительная простота и надежность их автоматического выявления на записях реакций при использовании сенсоров относительно невысокой частоты. Кроме того, рандомизация стимула может быть выполнена за счет использования данных о траектории движения. Подобные данные могут синтезироваться псевдослучайным образом либо быть заранее построенными в достаточном количестве, например, на основе большой базы векторных изображений.

Сбор данных и предварительный анализ индуцируемых движений

С использованием описанного в [4] инструментального комплекса мы можем проводить эксперименты по отслеживанию реакций людей на самые разные визуальные стимулы.

Стимулы отрисовывались в левой части экрана в окне 1000×800 пикселей и представляли собой движущуюся красную точку на белом фоне. Реакции испытуемых регистрировались с помощью активного сенсора с частотой 90 Гц.

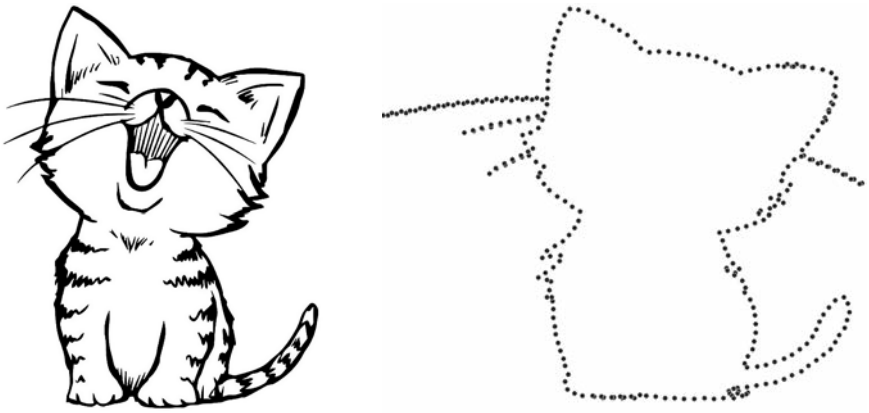

Рис. 1. ***Пример исходного изображения (слева), траектории демонстрируемого стимула (справа)***

Сбор данных производился в нескольких стационарных пунктах, что позволило в итоге получить достаточно крупный и разнообразный набор. В качестве траектории визуального стимула были использованы контуры векторных изображений животных (рис. 1). Всего было три уникальных контура: «cat», «kot#1» и «sobaka#1».

Стимулы демонстрировались на высокой и низкой скоростях движения точки.

Каждый тип стимула в комбинации со скоростью его воспроизведения имеет свой идентификатор, формирующийся следующим образом: «тип стимула» и «тип скорости». Например, «cat_slow» или «kot#1_slow». В дальнейшем при необходимости сослаться в тексте на конкретный стимул из набора мы будем использовать его идентификатор.

В данном эксперименте приняло участие 135 человек различного возраста (от 18 до 67 лет) и пола (50 женщин и 85 мужчин). Малая часть участников (порядка 3 % от общего числа) указала, что обладает некоторыми нарушениями зрения: дальнозоркость, миопия разной степени (от низкой – 0,5 диоптрий до несимметричной близорукости – 5 диоптрий), астигматизм, а также ношение контактных линз для корректировки зрения.

В общей сложности было записано 1826 сессий, пригодных для дальнейшего анализа, суммарной длительностью порядка 16 361 с (4 часа 32 минуты 41 секунда). На каждого участника приходилось от 1 до 23 записей. Средняя длительность записи зависела от вида используемого стимула: если его скорость высокая – от 6 до 33 с, иначе – от 18 до 42 с.

Для выделения следящих движений использовался специальный алгоритм классификации движений *Velocity and Dispersion Threshold Identification* (I-VDT) [12]. Согласно [13], при верном подборе порогов он имеет вероятность обеспечить результаты классификации, близкие к результатам, полученным с помощью ручной аннотации. I-VDT показывает малую чувствительность к изменчивости порогов и высокую устойчивость результатов при наличии в данных шумовой составляющей.

Саккады[1] в алгоритме I-VDT первыми извлекаются из записей взгляда как движения, характеризуемые высокой скоростью.

Порог скорости для саккад выбирался эмпирическим путем с учетом специфики изучаемых данных и известной частоты айтрекера[2] (90 Гц). В расчет принимались и биологические возможности глаза человека: длительность саккад обычно больше 12 мс и редко превышает 160 мс, кроме того, максимальная скорость, которую может развивать глаз при резком движении достигает 900°/с, од-

[1] *Саккада – быстрое одновременное движение обоих глаз между двумя или более фазами фиксации в одном направлении.*

[2] *Айтрекер – устройство, используемое для определения ориентации оптической оси глазного яблока в пространстве (то есть для отслеживания движения глаз).*

нако в большинстве случаев этот показатель располагается в диапазоне от 15 до 500°/с.

Два следующих параметра алгоритма – ширина временно́го окна обработки записи и порог дисперсии. Их подбор проводился экспериментально по сетке параметров с учетом длины и количества выявленных следящих движений. Кроме того, при оценке набора параметров учитывалось качество отделения колебаний записей взглядов при саккадах или моргании от плавных кривых в записи следящих движений.

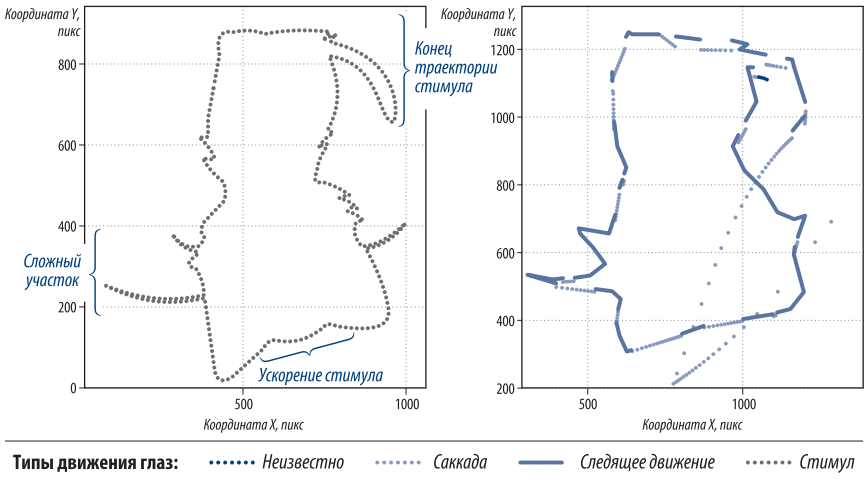

Рис. 2. ***Пример траектории движения стимула «cat_fast» (слева), траектории движения взгляда наблюдателя (справа)***

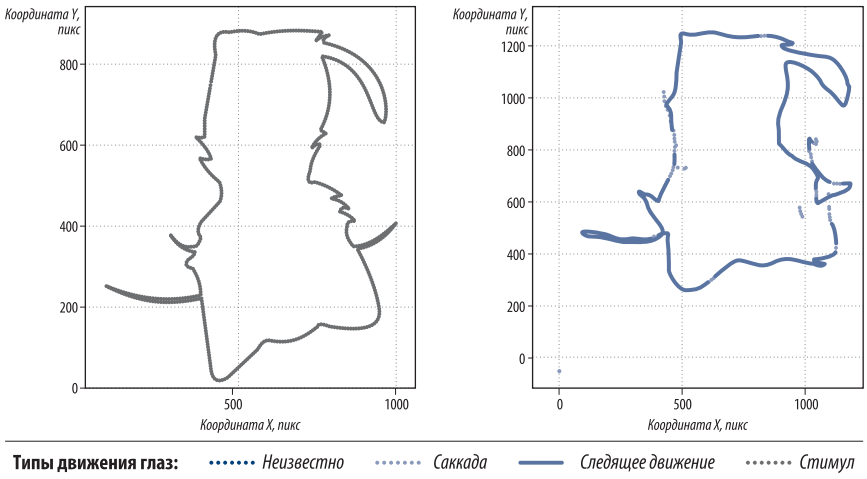

Рис. 3. ***Пример траектории движения стимула «cat_slow» (слева), траектории движения взгляда наблюдателя (справа)***

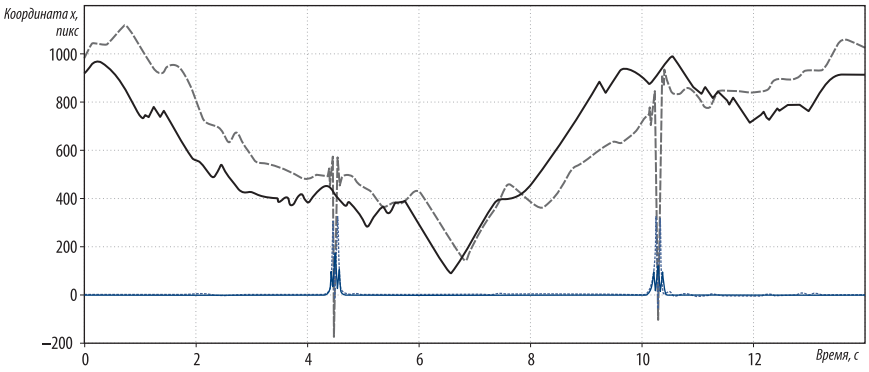

Рис. 4. ***График изменения координаты x взгляда (серая пунктирная линия), координаты стимула x (черная линия), скорости изменения положения взгляда (синяя пунктирная линия) и ускорения (синяя линия) для стимула типа «cat_slow»***

По результатам классификации с помощью алгоритма I-VDT суммарно во всех записях было обнаружено 20 702 саккады, 266 фиксаций и 20 895 следящих движений. Было получено следующее соотношение: 9 % от всех обнаруженных движений составляют саккады, 1 % – фиксации и 90 % – следящие движения, так как они имеют наибольшую протяженность. В среднем на каждую запись приходилось 12 коротких участков саккад, менее одной короткой фиксаций и 12 участков следящих движений.

Первичный анализ показал, что различные стимулы набора данных характеризуются различным качественным и количественным составом выявленных движений. Стимул «cat_fast» вызывал большее число саккад и следящих движений, чем остальные. Это вызвано, с одной стороны, более высокой скоростью движения точки, а с другой – усложненной траекторией, включающей резкие изменения направления движения стимула (рис. 2).

Траектории стимула на рис. 2 и в дальнейшем инвертированы по вертикали, поскольку построение произведено в координатной плоскости с естественным направлением роста по оси ординат, в то время как данные активного сенсора сформированы в стандарте отображения экранных координат с точкой начала в правом верхнем углу экрана.

Стимулы с низкой скоростью демонстрации провоцировали меньшее число саккад и фиксаций за счет более комфортного темпа движения точки. Например, траектория взгляда испытуемого, наблюдающего стимул «cat_slow», приведена на рис. 3, где заметно подавляющее число непрерывных следящих движений. А на диаграмме изменения координаты *x*, а именно скорости и ускорения ее изменения (рис. 4), можно отметить, что взгляд точно следует за точкой стимула с практически неизменной скоростью, однако имеет место небольшое отклонение в координатах плоскости экрана и запаздывание реакции глаза на долю се-

кунды. Также видны два сильных колебания на четвертой и на десятой секундах, которые иллюстрируют моргания наблюдателя.

Общая структура модели верификации и определение ее параметров

Любая модель идентификации/верификации человека должна иметь в своей основе совокупность качественных и количественных признаков, позволяющих отличать реакции разных людей и в то же время определять реакции одного и того же человека. Иногда удается выявить достаточную совокупность характерных признаков явным образом [9–11]. В этом случае можно говорить о явном или ручном способе построения признакового пространства.

Для задачи идентификации человека по особенностям движения глаз при слежении за динамическим стимулом явное признаковое пространство на сегодняшний день в литературе не описано. Предпринятые нами попытки его построить показали, что, с одной стороны, информация, позволяющая идентифицировать человека, в этих данных содержится, но, с другой стороны, качество работы такой модели не слишком высоко.

Альтернативой этому подходу является неявное построение пространства характерных признаков, например, с помощью применения искусственных нейронных сетей. В процессе нашего исследования удалось построить процедуру обучения нейронных сетей для решения задачи верификации на собранном наборе данных относительно небольшого размера, а также провести оценку качества с использованием специальной контрольной выборки, куда входили записи тех субъектов, с которыми модель на стадии обучения никак не взаимодействовала.

Очевидно, что в качестве объекта верификации в целом должна была бы выступать пара стимула и соответствующей реакции человека, которая по своей сути является временным рядом наблюдений четырехмерного сигнала. Тогда задача верификации сводится к поиску метрики сходства между парой временных рядов, такой, которая бы позволяла выделять индивидуальные характеристики зрительной реакции смотрящего, а не траекторию визуального стимула или влияние внешних факторов.

В данном случае предпочтительными становятся сверточные нейросетевые архитектуры, основанные на концепции самостоятельного выбора необходимого набора и иерархии абстрактных признаков, которые отфильтровывают маловажные детали и при этом выделяют существенное [14–16].

Обучение метрики сходства с помощью нейронных сетей подразумевает получение такого эффективного представления входных данных в метрическом пространстве высокой размерности, которое бы располагало заранее определенные схожие объекты относительно ближе друг к другу, чем различающиеся. Формально этот подход можно определить, задав семейство функций обработки $G_W(X)$, которые имеют параметры W и заранее обозначенную метрику сходства между экземплярами данных X_i и X_j, в общем случае описываемую выражением (1).

$$E_W(X_i, X_j) = g(G_W(X_i), G_W(X_j)), \quad (1)$$

где g – некоторая метрика сходства, например, евклидова, а $E_W(X_i, X_j)$ – показатель сходства двух объектов, скаляр.

Значение выражения $E_W(X_i, X_j)$ при условии принадлежности экземпляров данных X_i и X_j одному классу много больше, чем в ином случае. Обучение метрики происходит через определение наилучших параметров W для получения векторов, тесно сгруппированных по классовым признакам в пространстве. Получаемые таким образом многомерные векторы называются представлениями (*англ.* – embeddings) исходных данных во внутреннем признаковом пространстве модели.

Мы исследовали возможность применения основных подходов к построению архитектур, используемых сейчас в области глубокого обучения, а именно:

- сиамскую нейронную сеть с контрастивной функцией потерь (*Siamese Network with Contrastive loss*) [17];
- тройную нейронную сеть с триплетной функцией потерь (*Triplet Network*);
- прототипическую нейронную сеть (*Prototypical Networks*) или сети соответствия (*Matching Networks*) [18].

Мы провели эксперименты с моделями верификации, основанными на каждой из них. Но прежде чем перейти к результирующим оценкам качества, следует обратить внимание на то, что для обучения любой модели глубокого обучения требуется большое количество данных. Задача верификации могла бы решаться за счет подачи на вход одной из описанных выше нейросетевых структур пары:

- биометрического шаблона (построенного по эталонной паре «стимул – реакция» одного человека) и исследуемой записи;
- вычислении метрики сходства и принятии решения, основанного на сравнении с пороговым значением.

Однако для обучения подобных моделей требуется объем данных, существенно превышающий количество записей, которые пока удалось собрать в рамках наших экспериментов. Кроме того, полные записи, как уже отмечалось, содержат данные о движениях глаз разных видов, что усложняет сигнал и, соответственно, требует больше времени на обучение и еще большего объема обучающей выборки. В случае конкретных стимулов и реакции такая схема заставит нейросеть учитывать особенности присутствующих в данных саккадических движений, что создает дополнительные факторы неопределенности.

Наша идея заключается в том, чтобы рассмотреть в качестве объекта верификации для нейросетевой модели каждое отдельное следящее движение. Поскольку в рамках одной записи реакции на плавный стимул таких движений оказывается несколько, подобный подход дает возможность на порядки увеличить объем обучающей выборки.

Кроме того, использование следящих движений позволяет не только повысить количество образцов

обучающей выборки, но и сократить размерность описания каждого из них. Дело в том, что в обычном случае пара «стимул – реакция» должна бы быть представлена на вход нейросетевой модели в виде четырехмерного временного ряда синхронизированного положения стимула и реакции. Если же используется основное свойство следящих движений, заключающееся в том, что глаза описывают приблизительно ту же траекторию, что и объект, за которым они следуют, то достаточно использования двухмерного ряда их разности (рис. 5).

В большинстве случаев участки следящих движений имеют сильно различающуюся длительность, поэтому было решено привести их к одинаковой протяженности τ, разделив более длительные участки на несколько частей и исключив из рассмотрения существенно более короткие (<0,85 • τ) как малоинформативные. Значение τ выбрано на основе верхнего квантиля распределения длин участков следящих движений и составляет в наших экспериментах 0,2 с.

Помимо этого, набор векторов следящих движений был стандартизирован, то есть приведен к нормальному распределению с нулевым математическим ожиданием и единичным значением стандартного отклонения.

Структура базовой нейросети, используемой нами в исследовании, представляет собой сверточную сеть с механизмом внимания с общим количеством параметров 288 324. В наших экспериментах наилучшим образом пока показала себя структура слоев (схематично отображена на рис. 6).

Общие структуры исследуемых архитектур сетей глубокого обучения метрики не модифицировались. На рис. 7 приводится используемая в работе архитектура прототипической нейронной сети.

Необходимость использовать характерные участки записей в качестве объектов верификации для нейросетевой модели позволяет существенно увеличить объем обучающей выборки и сократить размерность задачи, однако этот подход требует разработки отдельной процедуры для идентификации человека по полной записи с учетом результатов работы модели верификации каждого из ее участков.

Предложенная процедура верификации объекта по полной записи основана на векторной близости нейросетевых внутренних представлений отдельных участков следящих движений к некоторому центру кла-

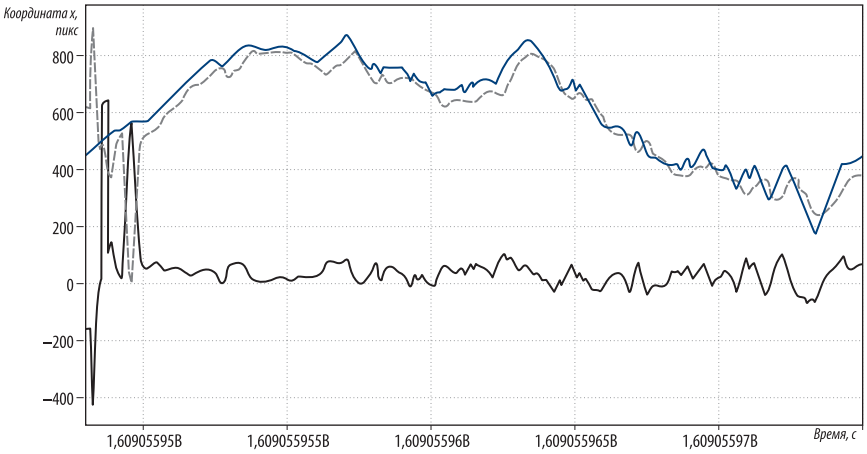

Рис. 5. ***Траектории движения стимула (синяя линия), взгляда (серая пунктирная линия) и отклонение (черная линия)***

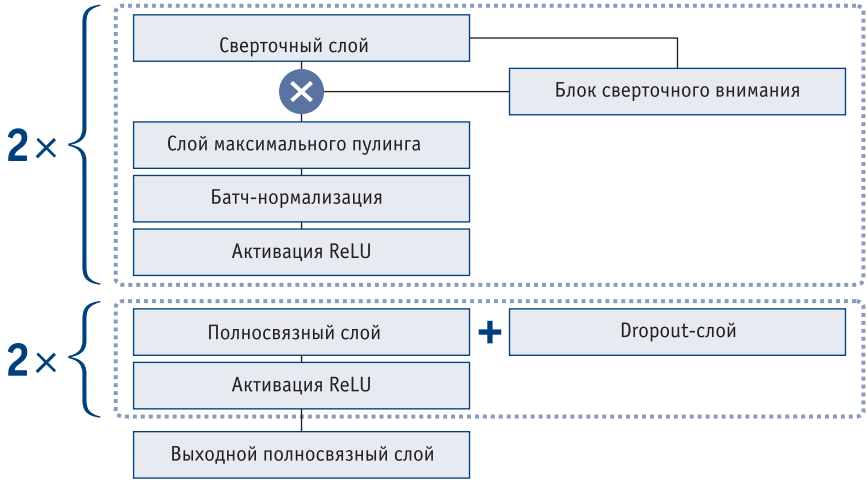

Рис. 6. ***Структура базовой нейросети G_w***

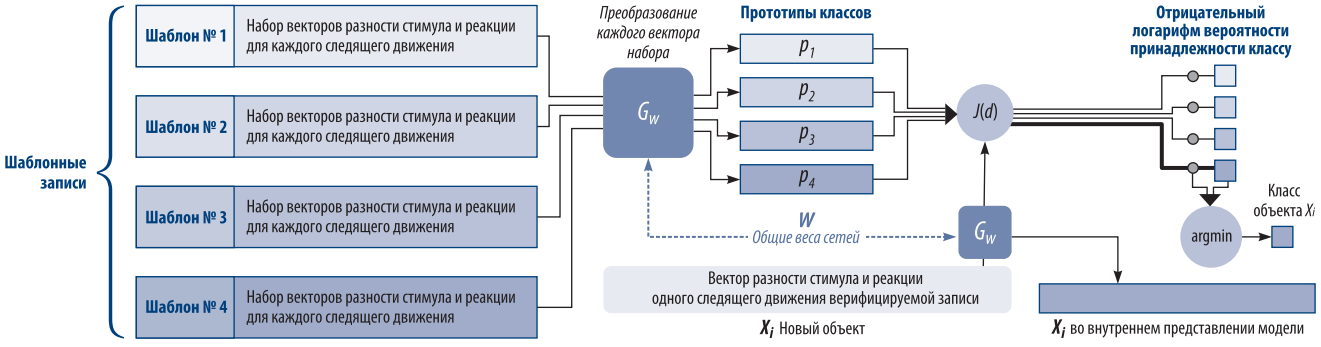

Рис. 7. ***Общая схема прототипической нейронной сети***

стера, сформированного аналогичными векторами представлений, относительно которых доподлинно известна их принадлежность верифицируемому субъекту. На рис. 8 эта схема проиллюстрирована графически, как завершающий этап в цепочке обработки верифицируемой пары «стимул – реакция».

Алгоритм агрегации основан на следующей идее: если медианы кластеров находятся достаточно близко друг к другу, возрастает вероятность принадлежности целой записи одному и тому же человеку (рис. 9); в ином случае значимые отличия в расположении кластеров означают, что между характеристиками двух рассматриваемых записей существуют отличия (рис. 10).

Таким образом, фактическое принятие решения о принадлежности новой записи верифицируемому человеку принимается на основе расчета разности между медианными векторами двух кластеров, сформированных признаковыми представлениями участков следящих движений каждой из записей взглядов.

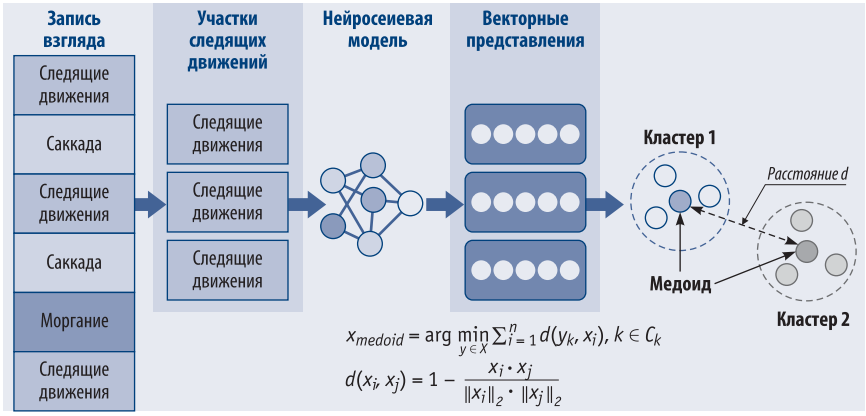

Рис. 8. ***Агрегация результатов оценки каждого следящего движения верифицируемой записи***

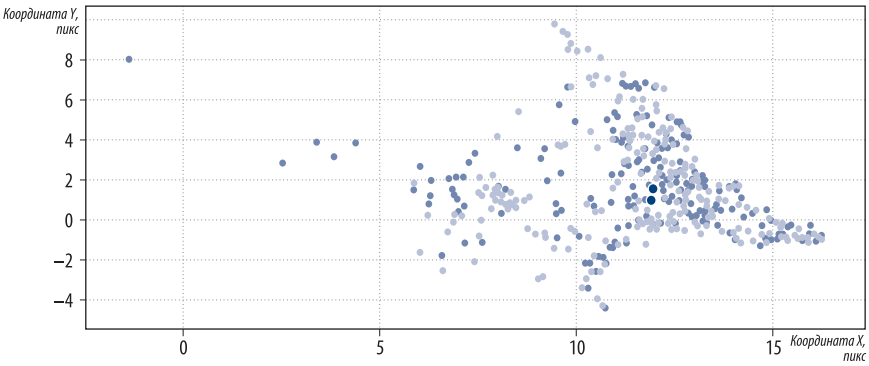

Рис. 9. ***Представления следящих движений двух записей одного и того же человека (в редуцированной размерности)***

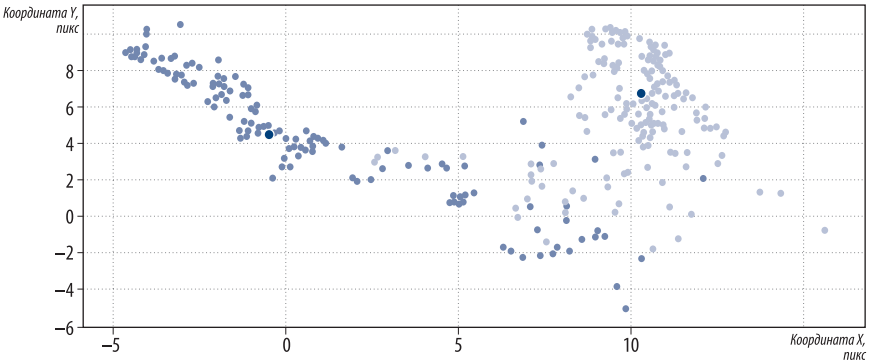

Рис. 10. ***Представления следящих движений двух записей разных людей (в редуцированной размерности)***

Оценка качества рассмотренных моделей

Для оценки количества ошибок моделей и соответствующих параметров качества мы делили исходный набор данных на четыре непересекающиеся подвыборки:

- обучающую;
- валидационную;
- «известную» тестовую, содержащую те записи, владелец которых также имеет несколько записей в составе обучающей выборки;
- «неизвестную» тестовую, куда попали исключительно записи тех участников эксперимента, которых не было в обучающей выборке.

Деление тестовых данных было выполнено для имитации с помощью последнего набора процесса валидации нового субъекта, записи которого не участвуют в формировании параметров и метапараметров модели, а также для сравнения разности качества результатов с «известными» тестовыми записями.

Для каждого из вышеприведенных наборов данных процентное и количественное соотношение целых записей в выборках различалось, но для чистоты экспериментальной статистики обучение и тестирование различных вариантов моделей производилось на одних и тех же записях.

Для каждого полученного таким образом тестового и валидационного набора следящих движений были созданы представления в векторном пространстве тестируемой модели. Затем с использованием валидационных наборов пар объектов были рассчитаны пороговые значения метрики расстояния между представлениями путем максимизации площади под кривыми качества (*Receiver Operating Characteristics curve*, ROC-AUC), причем предпочтительными значениями становились те, что минимизировали долю ложноположительных примеров (*False Positive Rate*, FPR) в результатах.

Заданное таким образом значение применялось для порогового преобразования расстояния между двумя представлениями в соответствующих тестовых выборках: если оно не превышало порога, делался вывод

о принадлежности участков одному человеку, иначе – разным людям.

На следующем этапе выделялись центроиды (пространственные медианы) кластеров представлений следящих движений, принадлежащих одной записи. Гистограмма на рис. 11 позволяет наглядно продемонстрировать на примере распределения расстояний между центроидами записей, принадлежащих одному человеку и разным людям, возможность выявления для этой меры расстояния порога верификации полной записи. Следует отметить, что диаграмма построена по «неизвестному» тестовому набору данных.

По «известной» и «неизвестной» тестовым выборкам построены оценки качества модели верификации.

Среди используемых ключевых процентных вероятностных показателей применялись:

- ложный допуск или «уровень требовательности системы» (*False Acceptance Rate*, FAR) – вероятность того, что система совершит ошибку, приняв любого иного человека за верифицируемого владельца записи взгляда;
- ложный отказ (*False Rejection Rate*, FRR) – вероятность того, что система совершит ошибку, не верифицировав самого владельца записи взгляда;
- макро F1-мера – макроусредненная оценка среднего гармонического между точностью (precision) и полнотой (recall);
- AUC-ROC – площадь под кривой ошибок (*Receiver Operating Characteristic*, ROC).

Соответствующие оценки качества ее работы для основных исследуемых архитектур приведены в таблице.

По показателям качества верификации человека по цельным сессиям записи взглядов также можно отметить, что модель прототипичной нейронной сети демонстрирует более перспективные результаты, чем другие подходы: *F*1-мера в среднем вдвое выше, а вероятность ложного отказа на порядок ниже, чем у остальных моделей, однако и показатель ложного допуска ниже, чем у триплетной сети.

Сравнение качества моделей между «известной» и «неизвестной» тестовыми выборками демонстрирует картину, подробная интерпретация которой требует дополнительных исследований. Однако можно отметить, что для прототипической нейросети наблюдаются малые изменения или рост значения показателя на «неизвестной» тестовой выборке, что может свидетельствовать о ее устойчивости, поскольку в целом она справляется с верификацией субъектов, информация о которых была ей недоступна в процессе обучения, не хуже, чем с теми субъектами, записи которых имели возможность попасть в обучающий или валидационный набор и, соответственно, были приняты в расчет при обучении параметров самой сети и в используемых на следующих стадиях пороговых значениях.

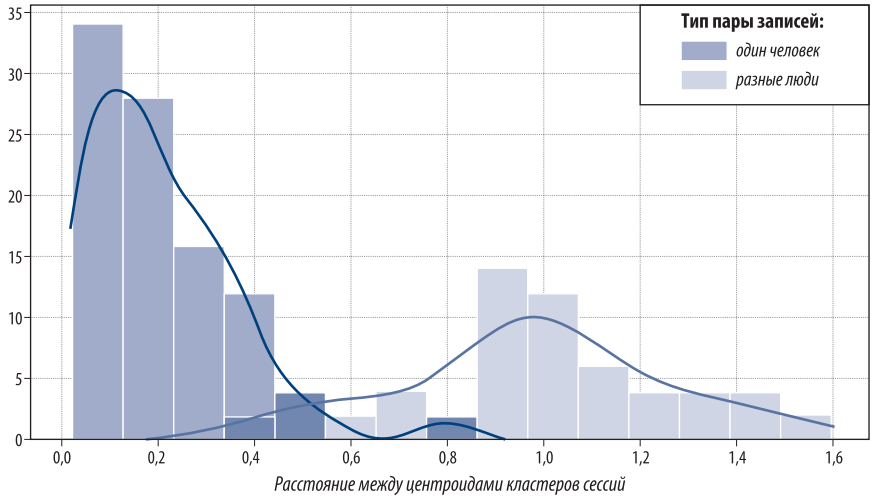

Рис. 11. ***Гистограмма расстояний между центроидами кластеров, соответствующих записям «неизвестной» тестовой выборки второго набора***

Таблица. ***Сравнение результатов верификации по целым записям взглядов***

Вероятностные показатели / Нейронная сеть	«Известная» тестовая выборка				«Неизвестная» тестовая выборка			
	FAR (%)	FRR (%)	Макро F1-мера	AUC-ROC	FAR (%)	FRR (%)	Макро F1-мера	AUC-ROC
Сиамская	5,46	45,54	0,41	0,552	12,55	38,32	0,45	0,506
Триплетная (тройная)	2,36	46,44	0,39	0,507	2,84	46,48	0,39	0,502
Прототипическая	8,70	8,10	0,83	0,909	9,58	1,48	0,89	0,963

Заключение

Показано, что даже при использовании сенсоров сравнительно невысокой частоты в данных о движении глаз достаточно информации, идентифицирующей человека. Этот факт позволяет с уверенностью говорить о возможности разработки промышленной технологии интерактивной биометрической идентификации, устойчивой к атакам на биометрическое представление. Техническими задачами на пути к разработке такой технологии являются сбор большого массива обучающих данных для повышения качества нейросетевых моделей, а также полноценный переход от использования активных сенсоров к пассивным камерам персонального компьютера или мобильного телефона.

Спектр открытых исследовательских вопросов в формирующейся области также весьма широк. Очевидно, что реализация самого способа идентификации будет совершенствоваться со временем. В частности, нашим коллективом уже ведется работа над автоматизацией подбора внутренних порогов предложенных алгоритмов, а также исследуются альтернативные способы финальной агрегации метрики расстояния. Кроме того, необходим экспериментальный анализ возможности создания атакующей генератив-

ной модели, оценка достижимого качества ее работы и необходимого объема обучающих данных для разработки методов защиты от целевых атак на используемые нейросетевые алгоритмы. ■

ЛИТЕРАТУРА

1. *Бродский А. В., Горбачев В. А., Карпов О. Э., Конявский В. А., Кузнецов Н. А., Райгородский А. М., Тренин С. А. Идентификация в компьютерных системах цифровой экономики // Информационные процессы. – 2018. – Т. 18, № 4. – С. 376–385.*
2. *Конявский В. А. Новая биометрия. Можно ли в новой экономике применять старые методы? // Information Security/Информационная безопасность. – 2018. – № 4. – С. 34–36.*
3. *Конявский В. А., Самосюк А. В., Тренин С. А. Рефлекторная биометрия для цифрового общества: первый шаг сделан // Information Security/Информационная безопасность. – 2020. – № 6. – С. 48–50.*
4. *Конявский В. А., Самосюк А. В., Тренин С. А., Петров С. Н., Абдуллаева И. А. Инструментальный комплекс анализа движения глаз для задач интерактивной рефлекторной идентификации // Защита информации. Инсайд. – 2021. – № 2 (98). – С. 18–22.*
5. *Гиппенрейтер Ю. Б. Движение человеческого глаза. – М.: Изд-во Моск. ун-та. – 1978.*
6. *Филин В. А. Автоматизация саккад. – М.: МЦ «Видеоэколдогия». Изд. Моск. ун-т. – 2001. – 263 с.*
7. *Vidal M., Pfeuffer K., Bulling A., Gellersen H. W. Pursuits: eye-based interaction with moving targets // CHI '13: CHI Conference on Human Factors in Computing Systems Paris France 27 April, 2013 – 2 May, 2013. NY. 2013. P. 3147–3150.*
8. *Cymek D. H. et. al. Entering PIN codes by smooth pursuit eye movements // Journal of Eye Movement Research. 2014. № 7 (4): 1. P. 1–11.*
9. *Bargary G. et. al. Individual differences in human eye movements: An oculomotor signature? // Vision Research. 2017. V. 141. P. 157–169.*
10. *Holland C., Komogortsev O. V. Biometric Identification via Eye Movement Scanpaths in Reading // IEEE International Joint Conference on Biometrics (IJCB). 2011. P. 1–8.*
11. *Kasprowski P., Harezlak K. Fusion of eye movement and mouse dynamics for reliable behavioral biometrics // Pattern Analysis and Applications. 2016. V. 21. P. 91–103.*
12. *Salvucci D. D., Goldberg J. H. Identifying fixations and saccades in eye-tracking protocols // ETRA '00: Proceedings of the 2000 symposium on Eye tracking research & applications. November 2000, NY. 2000. P. 71–78.*
13. *Komogortsev O. V., Karpov A. Automated classification and scoring of smooth pursuit eye movements in the presence of fixations and saccades // Behavior Research Methods. – 2013. – № 45 (1). – P. 203–215.*
14. *Krizhevsky A., Sutskever I., Hinton G. E. ImageNet classification with deep convolutional neural networks // Communications of the ACM. 2017. Vol. 60. № 6. P. 84–90.*
15. *Zeiler M. D., Fergus R. Visualizing and Understanding Convolutional Networks // Computer Vision – ECCV 2014. 2014. P. 818–833.*
16. *Shanmugam D., Blalock D., Guttag J. Jiffy: A Convolutional Approach to Learning Time Series Similarity. 2018.*
17. *Bromley J., Guyon I., LeCun Y. et. al. Signature verification using a siamese time delay neural network // International Journal of Pattern Recognition and Artificial Intelligence. 1993. № 7(04). P. 669–688.*
18. *Snell J., Swersky K., Zemel R. S. Prototypical Networks for Few-shot Learning // Advances in Neural Information Processing Systems 30 (NIPS 2017). 2017. Vol. 30. P. 1–11.*

НОВОСТИ

Вредоносы сегодня: редкие языки, новые тактики и атаки на виртуальные среды

Эксперты Positive Technologies проанализировали актуальные киберугрозы I квартала 2021 года и зафиксировали рост числа атак с помощью программ-вымогателей, появление множества новых шифровальщиков, а также отметили, что разработчики вредоносного ПО все чаще стали адаптировать его под атаки на средства виртуализации.

По данным анализа, количество атак увеличилось на 17 % в сравнении с I кварталом 2020 года, а относительно IV квартала 2020 года прирост составил 1,2 %. При этом 77 % атак были целенаправленными, а инциденты с частными лицами составили 12 % от числа всех происшествий. Главными целями злоумышленников в целом являются персональные и учетные данные, а при атаках на организации к ним добавляется коммерческая тайна.

Программы-вымогатели остаются самым распространенным вредоносным ПО. Их доля среди прочего вредоносного ПО, применяемого в атаках на организации, увеличилась на 7 % в сравнении с IV кварталом 2020 года и составляет 63 %. Эксперты также отметили появление новых шифровальщиков, например *Cring*, *Humble* и *Vovalex*.

Разработчики вредоносного ПО продолжают искать новые способы обхода средств защиты. Для этого они используют, к примеру, редкие языки программирования, как в случае с создателями вредоносного ПО для удаленного управления *BazarBackdoor*, которые переписали его, используя язык *Nim*, или операторами программ-вымогателей *Vovalex* и *RobbinHood*, которые изначально выбрали редкие языки *D* и *Golang*. Некоторые злоумышленники дополняют свои инструменты функциями, стирающими следы вредоносной активности.

По данным исследования, из-за того, что некоторые жертвы программ-вымогателей отказываются от уплаты выкупа, преступники все чаще угрожают сообщить о факте атаки и об украденных данных ее клиентам. По замыслу преступников, клиенты смогут повлиять на компанию и заставить ее заплатить, чтобы не допустить разглашения своих данных.

Все больше злоумышленников разрабатывают свои вредоносы для проведения атак на среды виртуализации, а некоторые пытаются активно эксплуатировать уже найденные уязвимости в ПО для развертывания виртуальной инфраструктуры. Прежде всего, эксперты связывают это с глобальным переносом ИТ-инфраструктуры компаний в виртуальную среду.

www.ptsecurity.com