ISSN 1684-8853 (print); ISSN 2541-8610 (online)

ИНФОРМАЦИОННО-УПРАВЛЯЮЩИЕ СИСТЕМЫ

НАУЧНЫЙ ЖУРНАЛ

2(129)/2024

doi:10.31799/1684-8853-2024-2

ISSN 1684-8853 (print); ISSN 2541-8610 (online)

SCIENTIFIC JOURNAL

2(129)/2024

PEER REVIEWED JOURNAL

INFORMATSIONNO-UPRAVLIAIUSHCHIE SISTEMY (INFORMATION AND CONTROL SYSTEMS)

Contact information
The Editorial and Publishing Center, SUAI
67A, Bol'shaya Morskaia, 190000, Saint Petersburg, Russia
Website: http://i-us.ru/en, e-mail: ius.spb@gmail.com
Tel.: +7 - 812 494 70 02

The Journal was registered in the Ministry of Press, Broadcasting and Mass Media of the Russian Federation.
Registration Certificate JD № 77-12412 from April, 19, 2002.
Re-registration in the Federal Service for Supervision in the Sphere of Telecom, Information Technologies and Mass Communications (ROSKOMNADZOR) due to change of the founder A. Vostrikov,
PI № FS 77-82226 from November, 23, 2021

Submitted for publication 11.03.24. Passed for printing 03.05.24. Signed for printing: 07.05.2024.
Format $60\times84_{1/8}$. Phototype CentSchbkCyrill BT. Digital printing.

Layout original is made at the Editorial and Publishing Center, SUAI.
67A, Bol'shaya Morskaia, 190000, Saint Petersburg, Russia
Printed from slides at the Editorial and Publishing Center, SUAI.
67A, Bol'shaya Morskaia, 190000, Saint Petersburg, Russia

The journal is indexed in Scopus.

Free distribution.

doi:10.31799/1684-8853-2024-2

ISSN 1684-8853 (print); ISSN 2541-8610 (online)

НАУЧНЫЙ ЖУРНАЛ

2(129)/2024

РЕЦЕНЗИРУЕМОЕ ИЗДАНИЕ

ИНФОРМАЦИОННО-УПРАВЛЯЮЩИЕ СИСТЕМЫ

Учредитель
А. А. Востриков
Издатель
Санкт-Петербургский государственный университет аэрокосмического приборостроения

Адрес редакции: 190000, г. Санкт-Петербург,
ул. Большая Морская, д. 67, лит. А, ГУАП, РИЦ
Тел.: (812) 494-70-02, эл. адрес: ius.spb@gmail.com,
сайт: http://i-us.ru

Журнал входит в БД Scopus и в Перечень рецензируемых научных изданий, в которых должны быть опубликованы основные научные результаты диссертаций на соискание ученой степени кандидата наук, на соискание ученой степени доктора наук.

Сдано в набор 11.03.24. Подписано в печать 03.05.24. Дата выхода в свет: 07.05.2024.
Формат 60×841/8. Гарнитура CentSchbkCyrill BT. Печать цифровая.
Усл. печ. л. 6,9. Уч.-изд. л. 9,4. Тираж 1000 экз (1-й завод 50 экз.). Заказ № 146.
Оригинал-макет изготовлен в редакционно-издательском центре ГУАП.
190000, г. Санкт-Петербург, ул. Большая Морская, д. 67, лит. А.
Отпечатано в редакционно-издательском центре ГУАП.
190000, г. Санкт-Петербург, ул. Большая Морская, д. 67, лит. А.
Распространяется бесплатно.

Журнал зарегистрирован в Министерстве РФ по делам печати, телерадиовещания и средств массовых коммуникаций.
Свидетельство о регистрации ПИ № 77-12412 от 19 апреля 2002 г.
Перерегистрирован в Роскомнадзоре.
Свидетельство о регистрации ПИ № ФС77-82226 от 23 ноября 2021 г.

УДК 519.614
doi:10.31799/1684-8853-2024-2-2-8
EDN: YOXUBL

Научные статьи
Articles

Опыт получения матриц максимума детерминанта бициклических структур на основе случайных последовательностей квантовой генерации

А. А. Востриков[a], *канд. техн. наук, доцент, orcid.org/0000-0002-8513-3683, vostricov@mail.ru*
А. М. Сергеев[a], *канд. техн. наук, доцент, orcid.org/ 0000-0002-4788-9869*
Ю. Н. Балонин[a], *научный сотрудник, orcid.org/0000-0002-5102-4139*
Д. В. Куртяник[a], *старший преподаватель, orcid.org/0000-0002-2895-6990*
К. Ю. Рыжов[a], *аспирант, orcid.org/0000-0002-8809-3218*
[a]*Санкт-Петербургский государственный университет аэрокосмического приборостроения, Б. Морская ул., 67, Санкт-Петербург, 190000, РФ*

Введение: *поиск матриц максимума детерминанта с двумя значениями элементов 1 и –1, являясь задачей трудоемкой, может быть упрощен внесением ограничений на их структуру. Поиск матриц на основе бициклических структур требует больших трудозатрат при подборе пар случайных последовательностей, порождающих блоки бицикла.* ***Цель:*** *показать развитие теории и обобщение семейств матриц максимума детерминанта при фиксации их структурных инвариантов. Проверить возможность получения максимальных размеров ортогональных последовательностей, которые можно извлечь при квантовой генерации для построения матрицы максимума детерминанта. Сопоставить случайные последовательности, получаемые из транспозонов в ДНК и с выхода квантового генератора.* ***Результаты:*** *предложено развитие теории и обобщение семейств матриц максимума детерминанта при фиксации их структурных инвариантов. Даны расширенные определения матриц оптимального дизайна, адамаридов, мерсеннидов и экстремальных бициклических структур. Введены определения плеча матрицы бициклической структуры и его размера. Описаны результаты проведенных компьютерных экспериментов с одним миллионом случайных последовательностей длины 100, сгенерированных на квантовом генераторе и позволивших получить ранее неизвестные матрицы максимума детерминанта на порядках, отличных от адамаровых.* ***Практическая значимость:*** *ортогональные матрицы и матрицы максимума детерминанта, являясь срезами ортогонального гиперобъекта, значительно расширяют семейство матриц Адамара, которые имеют большое практическое значение для задач ортогональных преобразований информации в телекоммуникациях.*

Ключевые слова *— квантовая генерация, случайные числа, случайные последовательности, матрицы максимума детерминанта, конструкции матриц, бициклические матрицы.*

Для цитирования: Востриков А. А., Сергеев А. М., Балонин Ю. Н., Куртяник Д. В., Рыжов К. Ю. Опыт получения матриц максимума детерминанта бициклических структур на основе случайных последовательностей квантовой генерации. *Информационно-управляющие системы*, 2024, № 2, с. 2–8. doi:10.31799/1684-8853-2024-2-2-8, EDN: YOXUBL
For citation: Vostrikov A. A., Sergeev A. M., Balonin Yu. N., Kurtyanik D. V., Ryzhov K. Yu. The experience of obtaining the maximum determinant matrices for two circulant structures based on quantum random number generation. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2024, no. 2, pp. 2–8 (In Russian). doi:10.31799/1684-8853-2024-2-2-8, EDN: YOXUBL

Введение

Матрицы максимального детерминанта, являясь математическим объектом многих научных исследований [1–5], сегодня уже не только представляют значительный научный или соревновательный интерес [6–9], но и широко используются при цифровой обработке информации в задачах помехозащищенного обмена по коммуникационным каналам, устойчивого корреляционного приема сигналов в системах связи и др. [10, 11]. Поэтому развитие теории и обобщение семейств матриц максимума детерминанта, в том числе при фиксации их структурных инвариантов, является задачей актуальной.

Матрицы максимального детерминанта — квадратные матрицы произвольных порядков n с элементами 1 и –1 — сходны с матрицами Адамара.

Матрицы Адамара [12, 13] $\mathbf{H}_n$ порядка n — матрицы с элементами 1 и –1, удовлетворяющие условию ортогональности $\mathbf{H}_n^{\mathrm{T}}\mathbf{H}_n = n\mathbf{I}_n$. Здесь $\mathbf{I}_n$ — единичная матрица того же порядка $n = 4t$, где t — натуральное число.

Матрицы Адамара имеют максимальный детерминант на указанных порядках $4t$. На порядках, открытых Голеем [14] и кратных, кроме 2, простым числам 5 и 13, матрицы Адамара представимы в виде бициклической конструкции

$$\mathbf{T}_n = \begin{pmatrix} \mathbf{A}_{n/2} & \mathbf{B}_{n/2} \\ \mathbf{B}_{n/2}^{\mathrm{T}} & -\mathbf{A}_{n/2}^{\mathrm{T}} \end{pmatrix},$$

где $\mathbf{A}_{n/2}$ и $\mathbf{B}_{n/2}$ — циклические матрицы, образуемые из последовательностей a и b длины $n/2$, размещаемых на месте их первых строк, после-

дующим их сдвигом в каждой следующей строке вправо и переносом последнего элемента на первую позицию в этой строке.

Матрицы Адамара сходны с матрицами максимального детерминанта с элементами 1 и –1 тем, что они также имеют максимальный детерминант. Однако порядки, на которых существуют матрицы максимального детерминанта, отличны от адамаровых, и эти матрицы могут быть не ортогональными [13, 14].

В задаче получения (построения) матриц Адамара и матриц максимума детерминанта большую роль играет способ получения последовательностей из 1 и –1, для чего используются случайная генерация, теория полей и групп, точки Гаусса на объектах вращения и др. [15, 16].

Первая матрица бициклической конструкции, отличная от голеевских, имеет порядок 68 (4×17), вторая — порядок 100 [17]. Внешне порядок 68 отличается увеличенным размером основы матрицы — 17.

Только для голеевских пар существует алгоритм перемножения их между собой [18, 19]. Отсюда следует, что находить не голеевские пары надо экспериментально, а это сводится к генерации случайных последовательностей.

Цель настоящей работы — показать влияние квантовой генерации случайных последовательностей на результативность поиска матриц максимума детерминанта с бициклическими структурами в основе.

Способы генерации случайных последовательностей

Получаемые с помощью программ на классическом компьютере случайные последовательности являются на самом деле псевдослучайными, имеющими ряд таких недостатков, как [20, 21]:

— ограниченный период, определяемый количеством последовательностей до начала воспроизводства одной и той же последовательности;

— зависимость последовательных значений, поскольку, как правило, вычисляются с использованием предыдущего значения генератора;

— обратимость — периодичность воспроизведения одной и той же последовательности и др.

Физические генераторы случайных чисел генерируют случайные последовательности за счет измерения параметров протекающих физических процессов [22–25]. В квантовой технике эти процессы, связанные с такими системами, как атомы, молекулы, элементарные частицы и т. п., являются идеальными источниками случайности.

Современные простые и недорогие генераторы случайных последовательностей (ГСП) построены, например, на использовании квантового оптического процесса. Такие квантовые генераторы формируют выходной случайный поток, в котором не наблюдается корреляций и выполняются все статистические тесты со скоростью до 10–16 Мбит/с [26]. ГСП на основе полупроводникового лазера с короткими и резкими пиками интенсивности [27] обеспечивают на выходе случайную последовательность со скоростью до 12,5 Гбит/с.

Более сложными и дорогими ГСП могут служить квантовые компьютеры (процессоры), такие как Advantage компании D-Wave (Канада) или Eagle компании USTC (Китай), в которых генерация случайных последовательностей реализуется за счет определения состояния множества кубитов при разрушении квантовой суперпозиции.

Семейства матриц Адамара

Элементарным обобщением матриц Адамара являются квазиортогональные матрицы со значениями пары элементов 1 и $-b$, удовлетворяющие условию $\mathbf{A}_n^{\mathrm{T}}\mathbf{A}_n = \omega\mathbf{I}_n$, где ω — целое или вещественное (рациональное, иррациональное) число.

Приведенное обобщение порождает семейство матриц Адамара, для которого бициклическая форма является универсальной [28]. Для матриц Адамара повышение порядка сказывается не на разрешимости, а на возможности поддерживать специфическую симметрию не самой матрицы, а операций с матрицами.

Приведем расширенные определения матриц семейства Адамара, введенные впервые в научный оборот в работе [28].

Определение 1. Матрицами оптимального дизайна (ОД) конструкции $\mathbf{T}_n$ четных порядков $4t - 2$ называют матрицы, сходные с матрицами Адамара тем, что среди матриц с ограниченными по величине элементами (не более единицы) они экстремальны — имеют самый большой детерминант.

Такие матрицы не могут быть ортогональными, это доказал Адамар, но они ортогонализуемы совместным изменением величины элементов одного знака. Иными словами, они не столь далеко отстоят от адамаровых и образуют с ними одно семейство оптимальных матриц.

Определение 2. «Адамаридами» будем называть матрицы порядков $4t + 1$, получаемые из адамаровых бициклов добавлением монотонной каймы из 1 в строке сверху и в столбце слева, первый (угловой) элемент которых равен –1.

Такие матрицы, кроме матриц на порядках, равных первым пяти числам Ферма, не строго оптимальны по детерминанту [29].

Определение 3. «Мерсеннидами» будем называть аналогичные матрицы порядков $4t - 1$, на единицу больших, чем порядки матриц ОД.

Однако следует отметить, что матрицы ОД существуют не всегда, тогда как экстремальные матрицы, построенные на основе бициклической структуры с каймой, существуют для всех порядков $4t - 1$. В них заведомо не входят порядки, равные числам, на единицу меньшим чисел Ферма, поскольку они принадлежат адамаридам.

Экстремальные бициклические матрицы

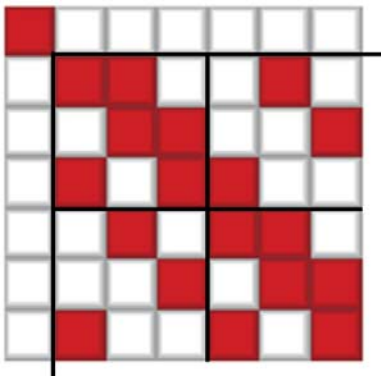
Строго оптимальные по детерминанту матрицы нечетных порядков, отличных от чисел Ферма, неограниченно усложняются с ростом порядков [15].

Определение 4. Плечом бицикла будем называть циклический блок $\mathbf{A}_{n/2}$ или $\mathbf{B}_{n/2}$, размер плеча составляет половину порядка бицикла — $n/2$. В настоящее время достоверно известна и доказана экстремальность матриц, не превышающих критического размера плеча 13.

Вполне ожидаемо, что на порядке 36 предполагаются проблемы поиска основы для наложения каймы, но они есть и для вполне безобидных голеевских порядков 32 и 64, поскольку 33 и 65 — не числа Ферма.

Ввиду резкого роста трудностей оправдан переход к более узкому классу матриц, экстремальных на бициклической структуре с каймой. Пример такой матрицы приведен на рис. 1, где выделены моноциклические блоки и кайма.

Здесь единичные элементы матрицы с положительным знаком представлены белым цветом, элементы с отрицательным знаком — красным цветом.



■ ***Рис. 1.*** Портрет бицикла с каймой
■ ***Fig. 1.*** Portraits of bicycle with border

Определение 5. Матрицу $\mathbf{T}_n$ будем называть экстремальным бициклом [28] в том случае, если она с нормализованной каймой

$$[\mathbf{T}_{n+1}] = \begin{pmatrix} -1 & \mathbf{e}^{\mathrm{T}} \\ \mathbf{e} & \mathbf{T}_n \end{pmatrix},$$

где все элементы вектора $\mathbf{e}$ равны единице, имеет максимум детерминанта на множестве матриц с такой структурой.

Уравнение орнамента матриц [15, 16] базируется на точках Гаусса сечения чаши параболоида $x^2 + y^2 = h$ на высотах h, где $h = n$ для матриц Адамара и $h = 2n - 2$ для матриц ОД. Однако ни матриц Адамара, ни матриц ОД бициклической конструкции может и не существовать. Например, нет бициклических матриц Адамара на порядках 36 и 72, хотя точки Гаусса имеются.

В том случае, когда нет точек Гаусса для заданного порядка, они определяются на высоте h, на которой существуют. Тогда задача сводится к выяснению: является ли это кольцо среза параболоида ближайшим или оно отстоит подальше.

Экстремальные бициклы и получаемые из них матрицы больших детерминантов нечетных порядков хорошо вписываются в общий контекст задачи на оптимальность и дополняют собой матрицы Адамара и ОД, отличаясь от них инвариантами $k_1 = (v - x)/2$, $k_2 = (v - y)/2$, задающими количество элементов со значением –1 в строках его плеч $\mathbf{A}_{n/2}$ и $\mathbf{B}_{n/2}$ размера v.

Для серий бициклических матриц на порядках Адамара в качестве опорных высот берутся размеры тех самых избранных семейств, куда вложены числа Ферма (минус единица, которая отвечает размеру каймы: 17 – 1 = 16 и т. п.). Отсутствие бицикла порядка 36 само по себе не мешает использовать этот порядок, на котором есть регулярные матрицы Адамара, но сложной структуры для расчета инвариантов серии бициклов. Инвариантами являются числа, а не матрицы. Невозможность ортогонализовать бицикл с такими параметрами для них не критична, поскольку ищутся заведомо неортогональные матрицы больших детерминантов.

Вслед за числом 36 для смещенных семейств такую же роль опорной высоты для расчета координат точек Гаусса играет порядок 64, хотя голеевская пара уступает блочной составной структуре с каймой. Тем самым для вычисления орнаментальных инвариантов используются ровно те же самые формулы, что и для матриц Адамара и ОД, но высота h в них соответствует влиятельному порядку, существенно отличному от порядка матрицы.

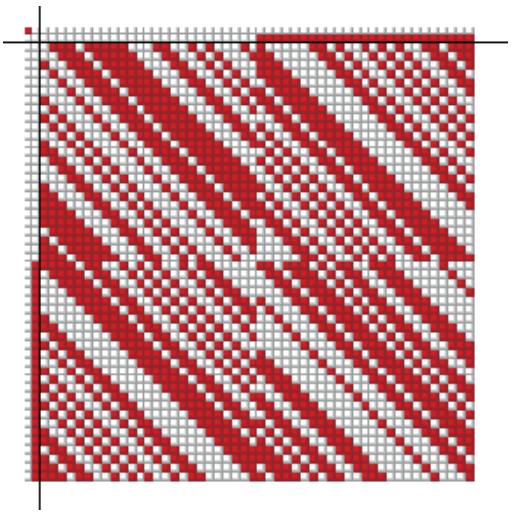
Установление величин инвариантов, характеризующих экстремальное решение, значительно сокращает алгоритмы поиска, поэтому приводимые здесь сведения являются новыми и важными.

Тест последовательности регулируемой длины

Использование случайных последовательностей для формирования ортогональных массивов или их блоков дает возможность судить по разрешимому порядку на выборке заданного объема о емкости массива случайных чисел из 1 и –1. На сегодня не известно о каких-либо работах по измерению емкости последовательностей в матрицах.

Кроме случайных последовательностей, полученных с квантового генератора, например на эффекте интерференции лазерных импульсов со случайной фазой [27], эксперименты для сравнения проводились и с биологическими последовательностями — с выборками из последовательностей Alu ДНК [30]. Длина таких последовательностей составляет всего 300 точек. Известно, что они формируют до 90 % генетического кода, играя специфическую роль скобок при переносах генетического материала. Скобка должна быть узнаваемой, поэтому от Alu получен высокий показатель «емкости» в матрицах.

Взяв сгенерированную квантовым способом 41 000 точек из чисел 1 и –1 и увеличивая в этом пределе выборку длины W = 1000, 2000 и т. п., можно наблюдать разрешимость данных бициклом Эйлера $\mathbf{T}_n$, являющимся основой матриц Адамара с двойной каймой (рис. 2). Симметрия бициклических структур [17] пока не учитывается.



■ ***Рис. 2.*** Портрет матрицы Адамара с бициклом Эйлера в качестве основы и с двойной каймой

■ ***Fig. 2.*** Portrait of Hadamard matrix with Euler bicycle and two borders

Из первых же экспериментов со случайными последовательностями стало ясно, что порядок 22 при заданных параметрах найти легко. Попытка подняться через четыре порядка выше по n приводит к критическому порядку 46, когда решение единственно и найти его можно увеличением объема данных. Это позволяет строить зависимость $n = f(\max(W))$ и следом прогнозировать нужные объемы данных.

Мерсенниды, описанные ранее, удобны тем, что их бицикл имеет такой же порядок, что и матрицы Эйлера, но они не ортогональны, и это гарантирует экстремальный детерминант для бицикла с каймой.

Если матрицы Эйлера — это типичный ортогональный базис при понижении уровня элемента со значением –1, то мерсенниды — базис из неортогональных векторов. Для них уже порядок 42 оказывается критичным. Ведут себя эти матрицы иначе: они имеют высокий эксцесс — бóльший разброс необходимых количеств 1 и –1. На порядке 42 этот разброс определяется значениями $k_1 = 11$ и $k_2 = 8$.

Обсуждение

Поскольку число паттернов (узоров) внутри ограниченной последовательности тоже ограничено, рано или поздно любая последовательность генератора исчерпывается. Кроме того, при равномерном выходе 1 и –1 с генератора случайных чисел возникает нарастающий с ростом порядка искомых матриц конфликт в различии эксцессов при поиске мерсеннидов, которого нет у биологических генераторов на основе ДНК.

Выход из этой ситуации видится в сложении двух последовательностей, получаемых с генератора случайных чисел и из последовательностей Alu ДНК. Получаемые при этом три уровня позволяют за единицу принимать один из них, меняя тем самым вероятность появления 1 и –1.

Использование такого способа позволило в частном эксперименте поднять разрешимый порядок мерсеннидов с 42 до 58, что ранее являлось недостижимым результатом при многочисленных поисках.

Однако такой способ сложения случайных последовательностей нельзя признать лучшим решением, хотелось бы иметь обратную связь на генератор случайных чисел. Это входит в общий вывод исследования.

Заключение

Использование квантовых ГСП и последовательностей Alu ДНК [30] как источников последовательностей с большим периодом и независимостью их фрагментов создает условия для продвижения в решении задач поиска новых ортогональных матриц и матриц максимума детерминанта.

Формирование широкого предложения таких матриц на различных порядках обеспечивает возможность лучшего выбора для задач обработки информации в телекоммуникационных системах и связи.

Описанный прием сложения двух случайных последовательностей позволяет менять как вероятность, так и разнообразие паттернов, искусственно расширяя выборку за счет времени работы генератора.

Анонсируя результаты выполненных исследований, мы не спешим с окончательными выводами, поскольку область нова и требует более тщательного исследования способов генерации случайных последовательностей и их влияния на результативность поиска матриц максимума детерминанта высоких порядков.

Благодарность

Авторы выражают благодарность сотруднику МИСиС Шаховому Роману за предоставленные для проведенных экспериментов случайные последовательности, сгенерированные в МИСиС в бинарном виде на квантовом генераторе «КуРэйт».

Финансирование

Работа выполнена при финансовой поддержке Министерства науки и высшего образования Российской Федерации, соглашение № FSRF-2023-0003 «Фундаментальные основы построения помехозащищенных систем космической и спутниковой связи, относительной навигации, технического зрения и аэрокосмического мониторинга».

Литература

1. **Ehlich H.** Determinantenabschätzungen für binäre Matrizen. *Mathematische Zeitschrift*, 1964, no. 83, pp. 123–132.
2. **Wojtas W.** On Hadamard's inequality for the determinants of order non-divisible by 4. *Colloquium Mathematicum*, 1964, vol. 12, pp. 73–83.
3. **Seberry J., Xia T., Koukouvinos C., Mitrouli M.** The maximal determinant and subdeterminants of ±1 matrices. *Linear Algebra and its Applications*, 2003, vol. 373, pp. 297–310. doi:10.1016/S0024-3795(03)00584-6
4. **Cohn J. H. E.** On determinants with elements ±1, II. *Bulletin of the London Mathematical Society*, 1989, no. 21, pp. 36–42.
5. **Neubauer M. G., Radcliffe A. J.** The maximum determinant of ±1 matrices. *Linear Algebra and its Applications*, 1997, no. 257, pp. 289–306.
6. **Brent R. R., Osborn J. H.** General lower bounds of maximal determinants of binary matrices: preprint, 2012. 15 p. arXiv:1208.1805
7. **Osborn J. H.** *The Hadamard Maximal Determinant Problem*: Honours thesis. University of Melbourne. http://maths-people.anu.edu.au/~osborn/publications/pubsall.html (дата обращения: 28.07.2023).
8. **Orrick W. P.** The maximal {−1, 1}-determinant of order 15. *Metrika*, 2005, no. 62, pp. 195–219.
9. **Orrick W. P., Solomon B.** Large determinant sign matrices of order 4k+1. *Discrete Mathematics*, 2007, no. 307, pp. 226–236.
10. **Wang R.** *Introduction to Orthogonal Transforms with Applications in Data Processing and Analysis*. Cambridge University Press, 2010. 504 p.
11. **Ahmed N., Rao K. R.** *Orthogonal Transforms for Digital Signal Processing*. Springer-Verlag Berlin Heidelberg, 2012. 264 p.
12. **Hadamard J.** Résolution d'une question relative aux déterminants. *Bulletin des Sciences Mathematiques*, 1893, vol. 17, pp. 240–246.
13. **Jennifer S., Yamada M.** *Hadamard Matrices: Constructions using Number Theory and Linear Algebra*. Wiley, 2020. 384 p.
14. **Colbourn C. J., Dinitz J. H.** *Handbook of Combinatorial Designs*. Second Ed. Chapman and Hall/CRC, 2007. 967 p.
15. **Балонин Н. А., Сергеев М. Б., Себерри Дж., Синицына О. И.** Окружности на решетках и матрицы Адамара. *Информационно-управляющие системы*, 2019, № 3, с. 2–9. doi:10.31799/1684-8853-2019-3-2-9
16. **Балонин Н. А., Сергеев М. Б., Себерри Дж., Синицына О. И.** Окружности на решетках и матрицы максимального детерминанта. *Информационно-управляющие системы*, 2020, № 6, с. 2–11. doi:10.31799/1684-8853-2020-6-2-11
17. **Балонин Н. А., Джокович Д. Ж.** Симметрия двуциклических матриц Адамара и периодические пары Голея. *Информационно-управляющие системы*, 2015, № 3, с. 2–16. doi:10.15217/issn1684-8853.2015.3.2
18. **Balonin N. A., Djocovich D. Z.** Negaperiodic Golay pairs and Hadamard matrices. *Информационно-*

управляющие системы, 2015, № 5, с. 2–17. doi:10.15217/issn1684-8853.2015.5.2

19. **Turyn R. J.** Hadamard matrices, Baumert — Hall units, four symbol sequences. pulse compression and surface wave encodings. *Journal of Combinatorial Theory*, 1974, no. 16, pp. 313–333.
20. **Иванов М. А., Чугунков И. В.** *Теория, применение и оценка качества генераторов псевдослучайных последовательностей*. М., Кудиц-образ, 2003. 240 с.
21. **Абросимов Д., Абросимова Е.** *Развитие графического способа тестирования псевдослучайной последовательности чисел.* Концепты хаоса и порядка в естественных и гуманитарных науках: монография. Нижний Новгород, Деком, 2011. С. 67–71.
22. **Манин Ю. И.** *Вычислимое и невычислимое.* М., Сов. радио, 1980. 128 с.
23. **Feyman R.** Simulating physics with computers. *International Journal of Theoretical Physics*, 1982, vol. 21, iss. 6–7, pp. 467–488.
24. **Benioff P.** Quantum mechanical hamiltonian models of turing machines. *Journal of Statistical Physics*, 1982, vol. 29, no. 3, pp. 515–546.
25. **Хвощ С. Т.** Матрицы Адамара как источник тестов квантовых компьютеров. *Инженерный вестник Дона*, 2023, № 3. www.ivdon.ru/ru/magazine/archive/n3y2023/8265 (дата обращения: 28.07.2023).
26. **Балыгин К. А., Зайцев В. И., Климов А. Н., Кулик С. П., Молотков С. Н.** Реализация квантового генератора случайных чисел, основанного на оптимальной группировке фотоотсчетов. *Письма в ЖЭТФ*, 2017, т. 106, № 7–8, с. 451–458. doi:10.7868/S0370274X17190109
27. **Shakhovoy R., Sych D., Sharoglazova V., Udaltsov A., Fedorov A., Kurochkin Y.** Quantum noise extraction from the interference of laser pulses in an optical quantum random number generator. *Optics Express*, 2020, vol. 28. iss. 5, pp. 6209–6224. doi:10.1364/OE.380156
28. **Балонин Н. А., Сергеев М. Б.** Максимум детерминанта бициклических матриц с каймой. *Информационно-управляющие системы*, 2023, № 3, с. 2–15. doi:10.31799/1684-8853-2023-3-2-15, EDN: JQPBFE
29. **Balonin N. A., Sergeev M. B., Vostricov A. A.** Prime Fermat numbers and maximum determinant matrix conjecture. *Информационно-управляющие системы*, 2020, № 2, с. 2–9. doi:10.31799/1684-8853-2020-2-2-9
30. **Хитринская И. Ю., Степанов В. А., Пузырев В. П.** Alu-повторы в геноме человека. *Молекулярная биология*, 2003, т. 37, № 3, с. 382–391.

UDC 519.614
doi:10.31799/1684-8853-2024-2-2-8
EDN: YOXUBL

The experience of obtaining the maximum determinant matrices for two circulant structures based on quantum random number generation

A. A. Vostrikov[a], PhD, Tech., Associate Professor, orcid.org/0000-0002-8513-3683, vostricov@mail.ru
A. M. Sergeev[a], PhD, Tech., Associate Professor, orcid.org/0000-0002-4788-9869
Yu. N. Balonin[a], Research Fellow, orcid.org/0000-0002-5102-4139
D. V. Kuryatnik[a], Senior Lecturer, orcid.org/0000-0002-2895-6990
K. Yu. Ryzhov[a], Post-Graduate Student, orcid.org/0000-0002-8809-3218
[a]Saint-Petersburg State University of Aerospace Instrumentation, 67, B. Morskaya St., 190000, Saint-Petersburg, Russian Federation

Introduction: The process of finding the maximum determinant matrices with two values of elements 1 and –1 being a laborious task, it can be simplified by introducing restrictions on their structure. Finding the matrices based on binary circulant structures is associated with the laborious selection of pairs of random sequences that generate two circulant blocks. **Purpose:** To show the development of the theory and generalization of families of maximum determinant matrices while fixing their structural invariants. To check the possibility of obtaining the orthogonal sequences of maximum sizes that can be extracted during quantum generation to construct a matrix of the maximum determinant. To compare random sequences obtained from transposons in DNA and from the output of a quantum generator. **Results:** We propose the development of the theory and generalization of families of maximum determinant matrices while fixing their structural invariants. We give extended definitions of optimal design matrices, hadamarides, mersennides and extremal two circulant structures. We introduce the definition for the arm of the matrix of the binary structure and its size. The results of computer experiments with 1 million random sequences of length 100 generated with a quantum generator are described, which allowed us to obtain previously unknown matrices of the maximum determinant on non-Hadamard orders. **Practical relevance:** Orthogonal matrices and matrices of the determinant maximum as the results of slices of an orthogonal hyperobject significantly expand the family of Hadamard matrices, which are of great practical importance for problems of orthogonal transformations of information in telecommunications.

Keywords — quantum generation, random numbers, random sequences, maximum determinant matrices, matrix constructions, two circulant matrices.

For citation: Vostrikov A. A., Sergeev A. M., Balonin Yu. N., Kurtyanik D. V., Ryzhov K. Yu. The experience of obtaining the maximum determinant matrices for two circulant structures based on quantum random number generation. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2024, no. 2, pp. 2–8 (In Russian). doi:10.31799/1684-8853-2024-2-2-8, EDN: YOXUBL

Acknowledments

The authors express their gratitude to the MISiS employee Shakhov Roman for providing random sequences generated in binary form on the KuRate quantum generator in MISiS for the experiments carried out.

Financial support

The paper was prepared with the financial support of the Ministry of Science and Higher Education of the Russian Federation, grant agreement No. FSRF-2023-0003.

References

1. Ehlich H. Determinantenabschätzungen für binäre Matrizen. *Mathematische Zeitschrift*, 1964, no. 83, pp. 123–132 (In German).
2. Wojtas W. On Hadamard's inequality for the determinants of order non-divisible by 4. *Colloquium Mathematicum*, 1964, vol. 12, pp. 73–83.
3. Seberry J., Xia T., Koukouvinos C., Mitrouli M. The maximal determinant and subdeterminants of ±1 matrices. *Linear Algebra and its Applications*, 2003, vol. 373, pp. 297–310. doi:10.1016/S0024-3795(03)00584-6
4. Cohn J. H. E. On determinants with elements ±1, II. *Bulletin of the London Mathematical Society*, 1989, no. 21, pp. 36–42.
5. Neubauer M. G., Radcliffe A. J. The Maximum determinant of ±1 matrices. *Linear Algebra and its Applications*, 1997, no. 257, pp. 289–306.
6. Brent R. R., Osborn J. H. General lower bounds of maximal determinants of binary matrices: preprint, 2012. 15 p. arXiv:1208.1805
7. Osborn J. H. *The Hadamard Maximal Determinant Problem*: Honours thesis. University of Melbourne. Available at: http://maths-people.anu.edu.au/~osborn/publications/pubsall.html (accessed 28 July 2023).
8. Orrick W. P. The maximal {−1, 1}-determinant of order 15. *Metrika*, 2005, no. 62, pp. 195–219.
9. Orrick W. P., Solomon B. Large determinant sign matrices of order 4k+1. *Discrete Mathematics*, 2007, no. 307, pp. 226–236.
10. Wang R. *Introduction to Orthogonal Transforms with Applications in Data Processing and Analysis*. Cambridge University Press, 2010. 504 p.
11. Ahmed N., Rao K. R. *Orthogonal Transforms for Digital Signal Processing*. Springer-Verlag Berlin Heidelberg, 2012. 264 p.
12. Hadamard J. Résolution d'une question relative aux déterminants. *Bulletin des Sciences Mathematiques*, 1893, vol. 17, pp. 240–246 (In French).
13. Jennifer S., Yamada M. *Hadamard Matrices: Constructions using Number Theory and Linear Algebra*. Wiley, 2020. 384 p.
14. Colbourn C. J., Dinitz J. H. *Handbook of Combinatorial Designs*. Chapman and Hall/CRC, 2007. 967 p.
15. Balonin N. A., Sergeev M. B., Seberry J., Sinitsyna O. I. Circles on lattices and Hadamard matrices. *Informatsionno-upravliaiushchie sistemy* (Information and Control Systems), 2019, no. 3, pp. 2–9 (In Russian). doi:10.31799/1684-8853-2019-3-2-9
16. Balonin N. A., Sergeev M. B., Seberry J., Sinitsyna O. I. Circles on lattices and maximum determinant matrices. *Informatsionno-upravliaiushchie sistemy* (Information and Control Systems), 2020, no. 6, pp. 2–11 (In Russian). doi:10.31799/1684-8853-2020-6-2-11
17. Balonin N. A., Djocovich D. Z. Symmetry of two-circulant Hadamard matrices and periodic Golay pairs. *Informatsionno-upravliaiushchie sistemy* (Information and Control Systems), 2015, no. 3, pp. 2–16 (In Russian). doi:10.15217/issn1684-8853.2015.3.2
18. Balonin N. A., Djocovich D. Z. Negaperiodic Golay pairs and Hadamard matrices. *Informatsionno-upravliaiushchie sistemy* (Information and Control Systems), 2015, no. 5, pp. 2–17. doi:10.15217/issn1684-8853.2015.5.2
19. Turyn R. J. Hadamard matrices, Baumert — Hall units, four symbol sequences. pulse compression and surface wave encodings. *Journal of Combinatorial Theory*, 1974, no. 16, pp. 313–333.
20. Ivanov M. A., Chugunkov I. V. *Teoriya, primenenie i ocenka kachestva generatorov psevdosluchajnyh posledovatel'nostej* [Theory, application and quality assessment of pseudorandom sequence generators]. Moscow, Kudic-obraz Publ., 2003. 240 p. (In Russian).
21. Abrosimov D., Abrosimova E. *Razvitie graficheskogo sposoba testirovaniya psevdosluchajnoj posledovatel'nosti chisel*. In: *Koncepty haosa i poryadka v estestvennyh i gumanitarnyh naukah* [Development of a graphical method for testing a pseudorandom sequence of numbers. In: Concepts of chaos and order in natural sciences and humanities]. Nizhnij Novgorod, Dekom Publ., 2011, pp. 67–71 (In Russian).
22. Manin Yu. I. *Vychislimoe i nevychislimoe* [*Computable and non-computable*]. Moscow, Sovetskoe radio Publ., 1980. 128 p. (In Russian).
23. Feyman R. Simulating physics with computers. *International Journal of Theoretical Physics*, 1982, vol. 21, iss. 6–7, pp. 467–488.
24. Benioff P. Quantum mechanical hamiltonian models of turing machines. *Journal of Statistical Physics*, 1982, vol. 29, no. 3, pp. 515–546.
25. Khvoshch S. T. Hadamard matrices as a source of quantum computer tests. *Engineering Journal of Don*, 2023, no. 3 (In Russian). Available at: www.ivdon.ru/ru/magazine/archive/n3y2023/8265 (accessed 28 July 2023).
26. Balygin K. A., Zajcev V. I., Klimov A. N., Kulik S. P., Molotkov S. N. Implementation of a quantum random number generator based on optimal grouping of photo reports. *JETP Letters*, 2017, vol. 106, no. 7–8, pp. 451–458 (In Russian). doi:10.7868/S0370274X17190109
27. Shakhovoy R., Sych D., Sharoglazova V., Udaltsov A., Fedorov A., Kurochkin Y. Quantum noise extraction from the interference of laser pulses in an optical quantum random number generator. *Optics Express*, 2020, vol. 28, iss. 5, pp. 6209–6224. doi:10.1364/OE.380156
28. Balonin N. A., Sergeev M. B. Maximum determinant two circulant matrices with border. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2023, no. 3, pp. 2–15 (In Russian). doi:10.31799/1684-8853-2023-3-2-15, EDN: JQPBFE
29. Balonin N. A., Sergeev M. B., Vostricov A. A. Prime Fermat numbers and maximum determinant matrix conjecture. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2020, no. 2, pp. 2–9. doi:10.31799/1684-8853-2020-2-2-9
30. Khitrinskaya I. Yu., Stepanov V. A., Puzyrev V. P. Alu repeats in the Human Genome. *Molecular Biology*, 2003, vol. 37, no. 3, pp. 325–333.

UDC 004.9
doi:10.31799/1684-8853-2024-2-9-20
EDN: XSSHJI

Articles

Deep learning-based IoT system for fruit and vegetable recognition

Pham Cong Thang[a], *PhD, Lecturer, orcid.org/0000-0002-6428-102X, pcthang@dut.udn.vn*
Nguyen Van Dung[a], *Student, orcid.org/0009-0004-1282-184X*
Le Tuan Nguyen Khoi[a], *Student, orcid.org/0009-0001-1191-2502*
Pham Duy Tin[a], *Student, orcid.org/0009-0002-2314-1503*
Tran Thi Thu Thao[b], *M. Sc., Lecturer, orcid.org/0000-0001-7705-2405*
[a]*The University of Danang — University of Science and Technology, 54 Nguyen Luong Bang St., Da Nang 550000, Vietnam*
[b]*The University of Danang — University of Economics, 71 Ngu Hanh Son St., Da Nang 550000, Vietnam*

Introduction: *In the context of the increasing importance of vegetables and fruits as essential nutritional sources, the demand for advanced computer vision-based fruit recognition technology within the supply chain has surged. This technology is critical at various stages, including harvesting, grading, and quality control.* ***Purpose:*** *To develop advanced fruit recognition systems through the integration of IoT devices, such as cameras and sensors, with deep learning algorithms.* ***Results:*** *This research utilizes convolutional neural networks to enhance fruit recognition capabilities by capturing intricate image features. We feed images of vegetables and fruits into pre-trained deep learning models to extract their deep features. Among these models, ResNet152V2 is notable for its robustness against noise and distortions, which makes it suitable for real-world applications. Its scalability allows it to handle larger datasets and more complex tasks, consistently achieving high accuracy in recognizing fruits and vegetables, even under challenging conditions. The dataset comprises around 31,000 images, spanning a diverse array of fruits and vegetables. The training process utilizes techniques like GlobalAveragePooling2D, fully connected layers, dropout for overfitting prevention, and softmax activation, culminating in an impressive accuracy of 98.01% for ResNet152V2 after 20 epochs. This surpasses the performance of a basic convolutional neural network model, which achieves 88.3%. Notably, when deployed on mobile platforms and Raspberry Pi 4, identification times are recorded at 4.3 seconds and 2.25 seconds, respectively. Concurrently, we develop both application software and an Internet of Things hardware system to monitor and enhance the fruit and vegetable recognition process.* ***Practical relevance:*** *The research addressed the fruit and vegetable recognition challenge by employing the ResNet152V2 deep learning model along with a dataset sourced from online and field channels. It achieved high accuracy, swift time series prediction, and the development of cost-effective, durable Internet of Things application hardware.*

Keywords *— fruit and vegetable recognition, deep learning, machine learning, ResNet152V2.*

For citation: Pham C. T., Nguyen V. D., Le T. N. K., Pham D. T., Tran T. T. T. Deep learning-based IoT system for fruit and vegetable recognition. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2024, no. 2, pp. 9–20. doi:10.31799/1684-8853-2024-2-9-20, EDN: XSSHJI

Introduction

Vegetables and fruits are important food sources for humans, providing essential nutrients such as vitamins, minerals, fiber, and antioxidants, which can positively impact human health [1–3]. In contemporary times, there has been a notable surge in the demand for fruit consumption, necessitating the adoption of modern production and processing techniques. Consequently, fruit recognition technology has emerged as a pivotal component within the fruit supply chain, finding applications at various stages. During the harvesting phase, it aids farmers in pinpointing the optimal time for harvest, thereby ensuring the superior quality of fruits. Moreover, during the grading phase, fruit recognition facilitates the categorization of fruits based on factors such as type, size, and ripeness, thus streamlining the transportation and storage processes. Finally, during the quality control phase, this technology plays a crucial role in identifying surface defects on fruits, thereby upholding food safety standards. The integration of deep learning techniques and robotic systems to automate agricultural processes has garnered considerable interest [4]. Fruits often thrive in complex environments fraught with uncertainty, making a robust fruit vision detection system imperative for smart agriculture and automated harvesting. The primary attributes of such a system include image sensors and fruit image data. Typically, fruit vision detection systems undergo five stages: image acquisition, preprocessing, feature extraction, segmentation, and recognition. Although still under development, these systems have the potential to revolutionize the agricultural industry. As the technology continues to improve, fruit vision detection systems are likely to become more widely used in agricultural applications [5, 6].

Additionally, the Internet of Things (IoT) is revolutionizing the detection and recognition of vegetables and fruits by integrating advanced sensors and data analytics to enhance accuracy and efficiency in agriculture. IoT technologies enable real-time monitoring of fruit crops, assessing factors such as ripeness, size, and health directly from the field. This data is invaluable for optimizing harvest times and improving crop management. IoT systems facilitate automated harvesting by guiding robotic systems to pick ripe fruits, thereby reducing labor costs and increasing operational efficiency. With the help of IoT, farmers can also detect early signs of disease and pest infestation, allowing for timely interventions to protect their crops. As IoT continues to evolve, its integration with artificial intelligence promises even greater advancements in automated fruit recognition and quality assessment, potentially transforming traditional farming practices into highly efficient, data-driven operations [7–9].

This research explores the utilization of convolutional neural networks (CNNs) to advance fruit recognition capabilities by acquiring intricate image features. We feed images of vegetables and fruits into pre-trained deep learning models to extract their deep features. Its scalability allows for handling larger datasets and more complex tasks, consistently achieving high accuracy in fruit and vegetable recognition, even under challenging conditions. Moreover, we evaluate the efficacy of deep features derived from various pre-trained deep learning models across different architectures for fruit and vegetable detection. Concurrently, we are developing both application software and an IoT hardware system to monitor and refine the fruit and vegetable recognition process.

Related work

The detection and recognition of fruits and vegetables is a multifaceted endeavor that necessitates the integration of diverse methodologies [10]. Fruit and vegetable recognition methodologies can broadly be categorized into two groups: feature-based recognition methods and machine learning-based recognition methods. Feature-based methods identify fruits and vegetables using geometric, color, or texture features [11–16]. In contrast, machine and deep learning-based methods employ models trained on datasets of labeled fruit images. Recent years have seen the proposal of various machine learning-based recognition methods [17, 18], including advanced deep learning techniques such as YOLO [19, 20], Single Shot Multibox Detector [21, 22], AlexNet [23, 24], VGG [25, 26], MobileNet [27, 28], ResNet [29, 30], and R-CNN [31, 32]. Although fruit vision detection systems are still under development, they have the potential to revolutionize the agricultural industry, with their usage likely to expand as the technology improves [33, 34].

Additionally, the integration of IoT and deep learning technologies has led to the development of advanced fruit recognition systems, marking a significant breakthrough in fruit processing and monitoring. At the core of this system lies the synergy between IoT devices, such as cameras and sensors, and deep learning algorithms [35, 36]. These devices capture real-time data from orchards or processing lines, providing a continuous flow of information. This data, which includes images, size measurements, color profiles, and other relevant features, is processed by the deep learning models. Trained on extensive datasets containing labeled fruit images and metadata, these algorithms learn intricate patterns and associations crucial for accurate fruit recognition and classification. Through iterative processes, the models are fine-tuned and optimized to achieve high levels of accuracy and efficiency.

The system's real-time capabilities enable instant recognition and classification of various fruit types, facilitating tasks such as sorting, quality control, and inventory management [37, 38]. Moreover, its scalability allows it to handle increasing volumes of data and adapt to evolving requirements in the fruit processing industry. By automating labor-intensive tasks and minimizing errors, this technology enhances operational efficiency while reducing costs. Furthermore, by ensuring consistent quality standards across different batches of fruits, it minimizes wastage and maximizes market value. Leveraging IoT capabilities, the system provides comprehensive traceability of fruits throughout the supply chain, addressing food safety concerns and ensuring compliance with regulatory standards [39, 40]. Stakeholders can remotely access and monitor the system's performance, receiving real-time updates on fruit processing activities, quality assessments, and inventory levels. Additionally, the system's predictive analytics capabilities offer valuable insights and forecasts regarding fruit yields, market demand, and supply chain optimization. Seamlessly integrating with existing enterprise resource planning systems, it facilitates data exchange and synchronization, streamlining business processes. A user-friendly interface allows operators to interact with the system, visualize key metrics, and configure parameters according to specific requirements. Through ongoing feedback loops and data-driven insights, the system undergoes continuous improvement, enhancing its accuracy, efficiency, and adaptability over time. The fruit recognition system utilizing IoT and deep learning technologies not only revolutionizes the fruit processing industry but also

enhances productivity, quality assurance, and market competitiveness [41–46].

Materials and methods

Currently, the challenges in achieving high accuracy and speed in fruit recognition stem from several factors. These include the lack of quality assurance in fruit datasets, difficulties in detecting various types of fruit, limitations in the size and clarity of the target detection frame, and the use of lightweight fruit detection models. Collecting high-quality fruit datasets is a critically important task. These datasets act as foundational elements in training deep learning models, significantly influencing their post-training accuracy in fruit recognition. In the realm of deep learning-based fruit recognition, datasets must meet two essential criteria: sufficiency and diversity. Sufficiency means having an ample amount of data, while diversity refers to the variation in types of fruits and vegetables represented. Typically, fruit datasets are sourced from outdoor environments or online repositories. Moreover, it's crucial to ensure a proportional distribution of fruit and vegetable data during collection. Depending on the research focus, researchers select datasets that align with their specific requirements. Different datasets exhibit significant variations in the quantity, quality, and categories of images, as well as the types of fruits and vegetables included.

In this study, we utilized the Kaggle dataset, known for its popularity and extensive use. This dataset includes a total of 40 categories and a substantial number of images. However, it suffers from drawbacks such as single-image backgrounds, insufficient diversity, and category imbalances. Despite these limitations, the Kaggle dataset remains a valuable resource for research and development in fruit recognition tasks.

The dataset

The dataset for this study was aggregated from two sources: Fruit and vegetables (https://www.kaggle.com/datasets/shadikfaysal/fruit-and-vegetables-ssm) and Vegetable images (https://www.kaggle.com/datasets/misrakahmed/vegetable-image-dataset). It comprises a total of 31,000 images, which are divided into three subsets in an 8:1:1 ratio: the training dataset, the validation dataset, and the test dataset. Specifically, the training dataset includes 24,000 images, the validation dataset contains 3,500 images, and the test dataset also consists of 3,500 images (Fig. 1).

Since the data is compiled from various sources and the images are captured under unrealistic conditions, the pictures in reality will not always meet criteria such as angle, brightness, and size. Therefore, it is necessary to process the input data so that training the model can yield more accurate results reflective of real-world conditions.

Resize image: The data is compiled from various sources and varies in size. For model training, it's crucial that the input data adhere to a specific condition: the images must have matrix data of identical dimensions. In this case, we have chosen an image size of 224×224 for training the model. Using this size can reduce memory usage and increase computational efficiency, while still retaining essential information.

Image augmentation: In reality, images are always subject to varying lighting conditions and angles, so training should be supported by robust image data processing.

Rotation range: Randomly rotating images at various angles diversifies the data and helps the model generalize beyond the original dataset. This enhancement supports training across various angles and shooting techniques, improving the model's robustness.

Zoom range: Random zoom enables the creation of different versions of the same image, reducing the training model's dependence on a fixed size. This adjustment enhances both the accuracy and robustness of the model, more accurately reflecting real-world size variations.

Width shift range: In real-life images, objects may not always be centrally located but can appear in various positions. By randomly shifting the image horizontally, each shift creates a slightly offset version of the original, which helps the model better adapt to practical situations.

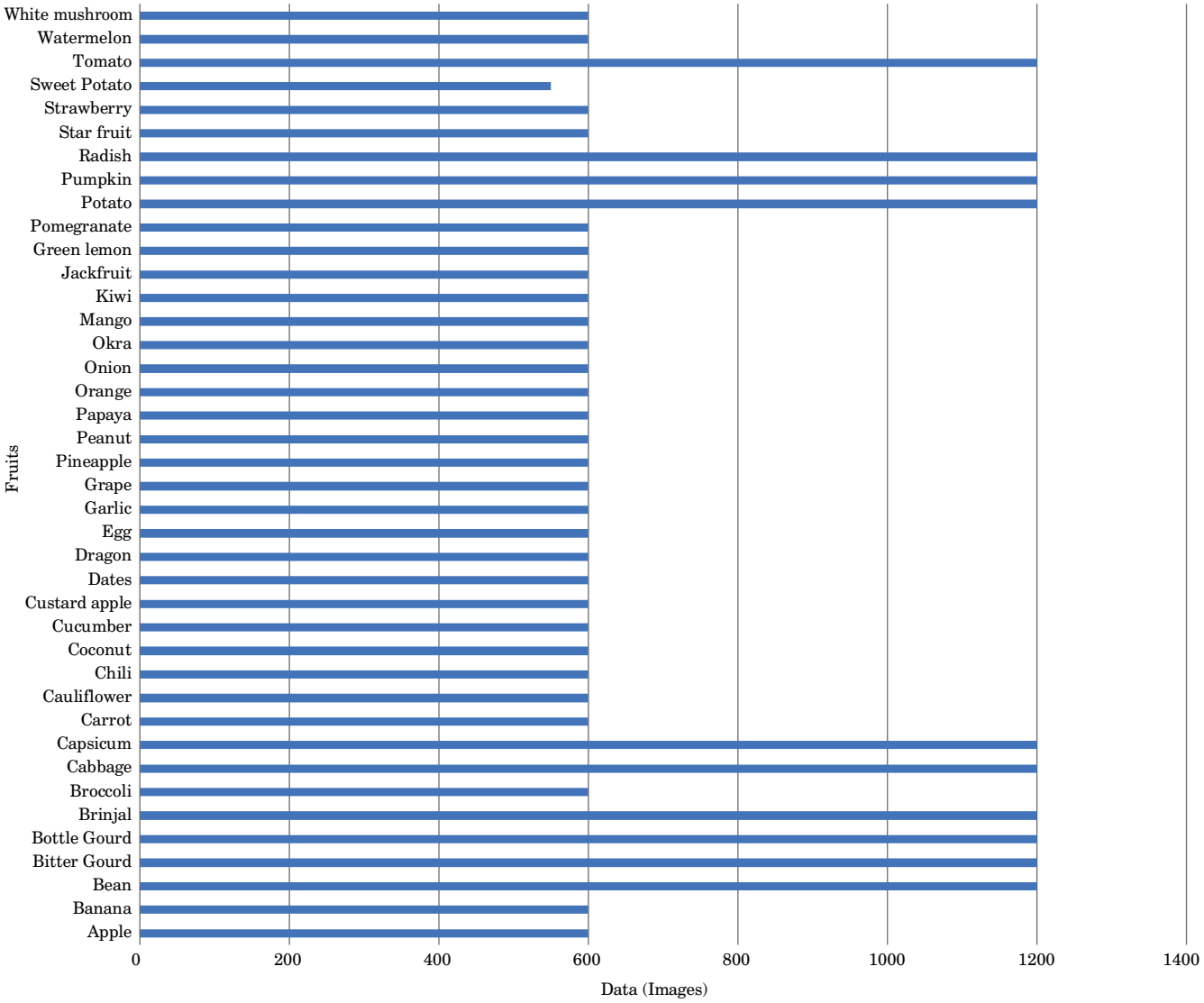
Brightness range: Randomly adjusting the brightness in images makes the data more representative of real-world conditions, thereby helping the model to become less dependent on specific lighting conditions.

Rescale: Rescaling pixel values from a range of 0–255 down to 0–1 stabilizes and enhances the efficiency of neural network training. This reduction helps prevent gradient saturation and explosion, stabilizes the backpropagation process, and accelerates the model's learning speed.

Deep learning model

In this work, we chose ResNet152V2 for data training [47]. ResNet152V2, an enhanced version of the original ResNet152, is a deep CNN architecture that features 152 layers (Fig. 2). It incorporates various improvements over its predecessor to enhance training convergence, reduce overfitting, and boost overall performance. Below is a detailed overview of the ResNet152V2 architecture.

Input layer: Accepts RGB images that are typically resized to a fixed dimension, such as 224×224 pixels.



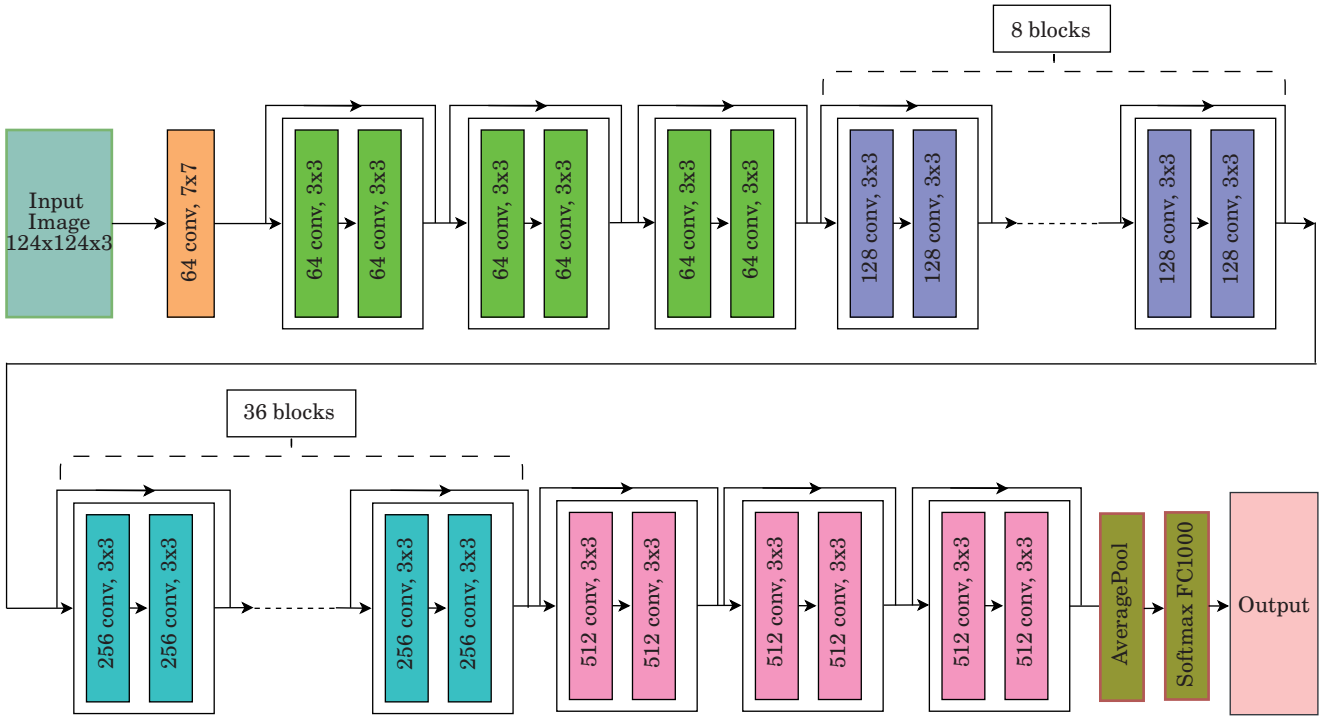
■ ***Fig. 1.*** Number of images for each fruit and vegetable

Initial convolutional layer: The input image undergoes an initial convolution; typically, this involves a 7×7 convolution with 64 filters, applied with a stride of 2. This step is followed by batch normalization and ReLU activation. After the initial convolution, a max-pooling layer with a 3×3 kernel and a stride of 2 is used to reduce the spatial dimensions of the feature maps. This sequence of steps marks the initial stage after the input layer, referred to as stage 1.

Residual blocks: ResNet152V2 consists of multiple residual blocks, each containing a stack of convolutional layers with skip connections [47]. These skip connections enable gradients to flow directly through the network, preventing them from vanishing. The residual blocks are grouped into stages, each containing a different number of blocks. The blocks within each stage have similar architectures but vary in the number of filters. In ResNet152V2, there are four stages, referred to as stages 2 to 5. The distribution of residual blocks across these stages is as follows: stage 2 includes 3 blocks with 64 filters; stage 3 has 8 blocks with 128 filters; stage 4 comprises 36 blocks with 256 filters; and stage 5 includes 3 blocks with 512 filters.

Global average pooling layer: After the final residual stage, global average pooling is applied to aggregate spatial information across the entire feature map. This operation effectively reduces the spatial dimensions to a single vector for each feature map, simplifying the output for further processing.

Fully connected layer: A fully connected layer, typically equipped with softmax activation, is added to neural network architectures for classification tasks. The number of neurons in this output layer corresponds directly to the number of classes in the



■ ***Fig. 2.*** Architecture of ResNet152V2

classification problem, providing a probability distribution across all possible outcomes.

Output layer: The output layer produces the final class predictions based on the softmax probabilities generated by the fully connected layer. This ensures that the output represents the likelihood of each class, allowing for the determination of the most probable category.

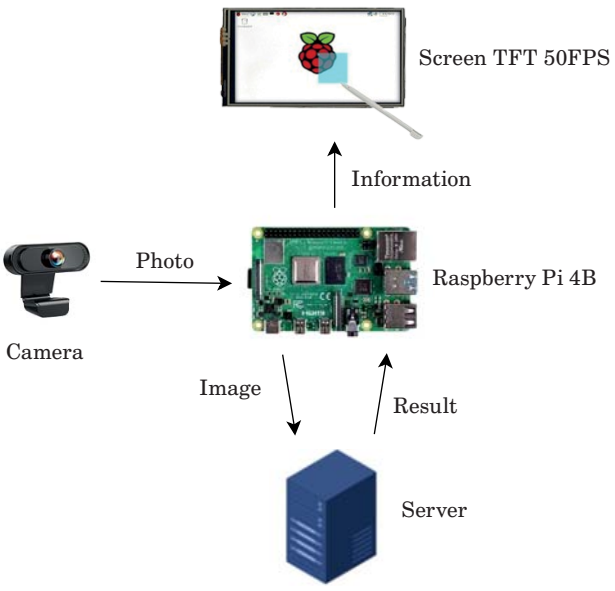
Overall, ResNet152V2's architecture enables the training of very deep neural networks while addressing issues such as vanishing gradients. It has demonstrated state-of-the-art performance on various image classification benchmarks and is widely used in research and applications that require high-performance computer vision models.

System design

We have developed a system to empirically evaluate the performance of a deep learning model in recognizing fruits and vegetables. The system consists of three main components: hardware, software, and an intermediary server, all of which are interconnected. A diagram of the system is depicted in Fig. 3.

Hardware: This setup includes a Raspberry Pi 4B board for processing, complemented by a screen and a camera. These components serve dual purposes: they not only facilitate the display of the user interface but also capture images for the recognition of vegetables and fruits. Furthermore, the hardware is designed to interact directly with the server, which enables data reception and streamlines the identification process.

Software: The software component is a mobile application developed using the React Native framework (JavaScript) [48]. The advantages of using React Native include the ability to develop applications for both iOS and Android from a single source code, significantly reducing development effort and costs. Additionally, applications built with React

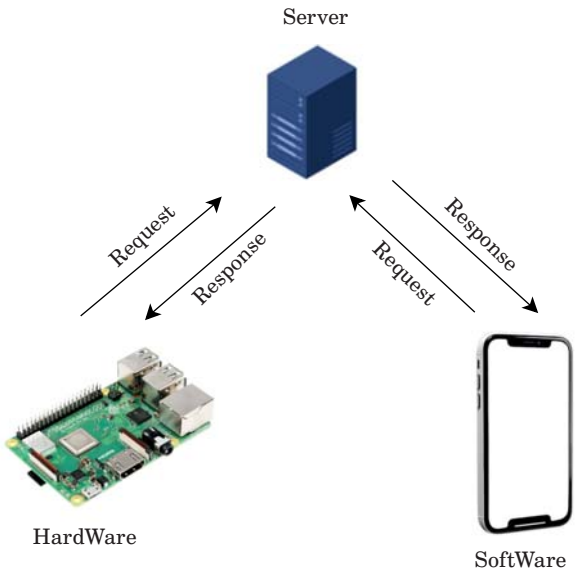


■ ***Fig. 3.*** The hardware circuit diagram

Native offer performance close to native apps due to optimizations and the ability to incorporate native components. The large and active React Native community provides extensive resources and support, aiding developers in promptly resolving issues. The framework's hot reloading feature allows developers to immediately see the effects of their changes, thereby streamlining the development and testing process (Fig. 4).

The software is directly linked to the server for data retrieval and for recognizing vegetables and fruits. Users can log into the system to perform fruit recognition, save recognized items or related dishes to their favorites list, and access their recognition history. Furthermore, our mobile application enables users to identify fruits and vegetables anywhere by capturing photos. Upon capturing an image, it is sent to the server for identification, and the server returns detailed information about the type of fruit or vegetable to the client. Each type of fruit or vegetable in the application is associated with a menu of dishes tailored to that specific product. This feature is designed to assist users in making informed dietary choices based on the identified fruits and vegetables.

Server: Our system utilizes two servers to optimize functionality. The first server, developed with NodeJS (JavaScript), supports user functionalities such as registration, login, storing recognition history, and maintaining records of recognized fruits/vegetables and preferred dishes. The second server, built with Flask (Python), focuses on the recognition of fruits and vegetables. For the mobile application component, we chose React Native (JavaScript) due to its numerous advantages over other programming languages. However, it is important to note that, despite its many benefits, we have encountered certain limitations during the development process.



■ ***Fig. 4.*** System diagram

In this study, we showcase an efficient application architecture that employs two servers simultaneously: one using NodeJS for database management and user connectivity, and another using Flask to host the recognition model and manage data prediction tasks. The integration of NodeJS and Flask offers significant advantages in developing web applications, particularly when addressing complex and diverse requirements. This dual-server setup allows for robust, scalable solutions that can efficiently handle both backend data management and real-time data processing tasks, as follows:

Performance and concurrent processing: Employing NodeJS for the database management server leverages its non-blocking architecture, optimizing performance and enabling concurrent processing when interacting with data from multiple sources. This capability is crucial, especially when prompt feedback from the database is essential for efficiently responding to user requests.

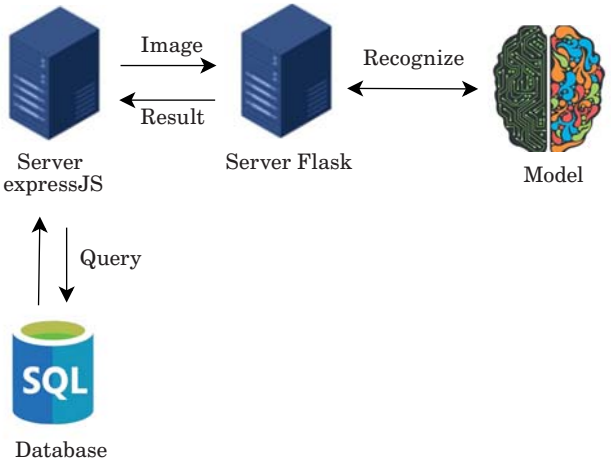
Work separation and flexibility in development: Using NodeJS for database management and Flask for hosting the model facilitates a natural separation of tasks. This division allows the development team to focus on database-related logic and data processing in NodeJS, while concurrently developing and maintaining the machine learning model in Flask.

Unified JavaScript and efficient interaction: Uniformity in using the JavaScript language across the NodeJS server and the browser simplifies data transmission and interaction between application components. This consistency enhances the efficiency of interactions between the database management server and the model-hosting server.

Fast feedback and real-time application: This architecture is ideal for applications requiring fast feedback and real-time processing. NodeJS, with its non-blocking architecture, excels in efficiently handling these requirements. Meanwhile, Flask's lightweight and flexible nature makes it convenient for deploying and maintaining the machine learning model.

Security and efficient resource management: The combination of NodeJS and Flask offers advantages in resource management and security. NodeJS, with its capability for efficient concurrent processing, helps alleviate pressure on system resources. Simultaneously, Flask's lightweight nature contributes to maintaining a high level of security.

In conclusion, the simultaneous use of NodeJS and Flask servers in our application architecture provides a robust solution for developing web applications with enhanced performance, clear task separation, and efficient interaction. This architecture is particularly advantageous for applications re-



■ ***Fig. 5.*** Server system architecture diagram

quiring real-time processing and aims to maintain a secure and resource-efficient system. The intermediary server architecture diagram is illustrated in Fig. 5.

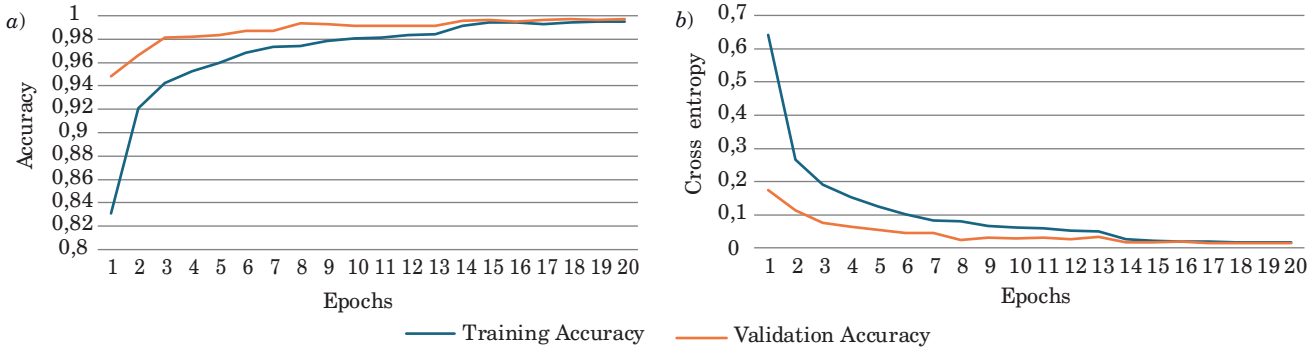
Results

Based on the designed system depicted in Fig. 3, the hardware configuration includes a Raspberry Pi 4B equipped with a 64-bit quad-core processor [49], two HDMI ports, two USB 2.0 ports, two USB 3.0 ports, one audio jack, and a MicroSD card slot. Additionally, it features a 5MP camera capable of capturing images at resolutions of 1080p and 720p, providing an image resolution of 2592×1944 pixels for 1080p and 1280×720 pixels for 720p. Complementing this is a 3.5-inch TFT screen with a resolution of 320×480 and a refresh rate of 50 FPS, integrated into the setup. The Raspberry Pi 4B connects to both the screen and the camera. Image data captured by the camera is transmitted to the Raspberry Pi 4B and displayed on the screen interface. Access to this interface is facilitated through a website hosted on a NodeJS server. Images are transmitted from the Raspberry Pi to the server for recognition, with the results subsequently displayed on the 50 FPS TFT screen. This setup enables real-time image recognition and display, making it suitable for various applications in scientific research and development (Fig. 6). Figure 7 shows the interface of the designed mobile application. The source code of the designed system can be accessed here (https://github.com/pacotha/DL_Based-IoT.git).

The deep learning model ResNet152V2 undergoes a training process consisting of approximately 20 epochs (Fig. 8, *a*, *b*), with a dropout rate of 0.2. This dropout rate leads to the disabling of neurons, resulting in the inevitable loss of information pertaining to each sample. Consequently, subsequent layers must rely on incomplete representations to formulate predictions. As a result of this loss, the training loss tends to increase, posing artificial challenges for the network in providing accurate answers. However, during the validation phase, all units remain accessible, allowing the network to leverage its complete computational capacity. This

■ ***Fig. 6.*** Hardware simulation of the system

■ ***Fig. 7.*** The interface of the designed mobile application



■ ***Fig. 8.*** Accuracy (*a*) and loss (*b*) after 20 epochs

■ ***Table 1.*** Comparison of optimizers and accuracy

Optimizer	Accuracy, %
Adam	95.3
RMSPROP	98.01

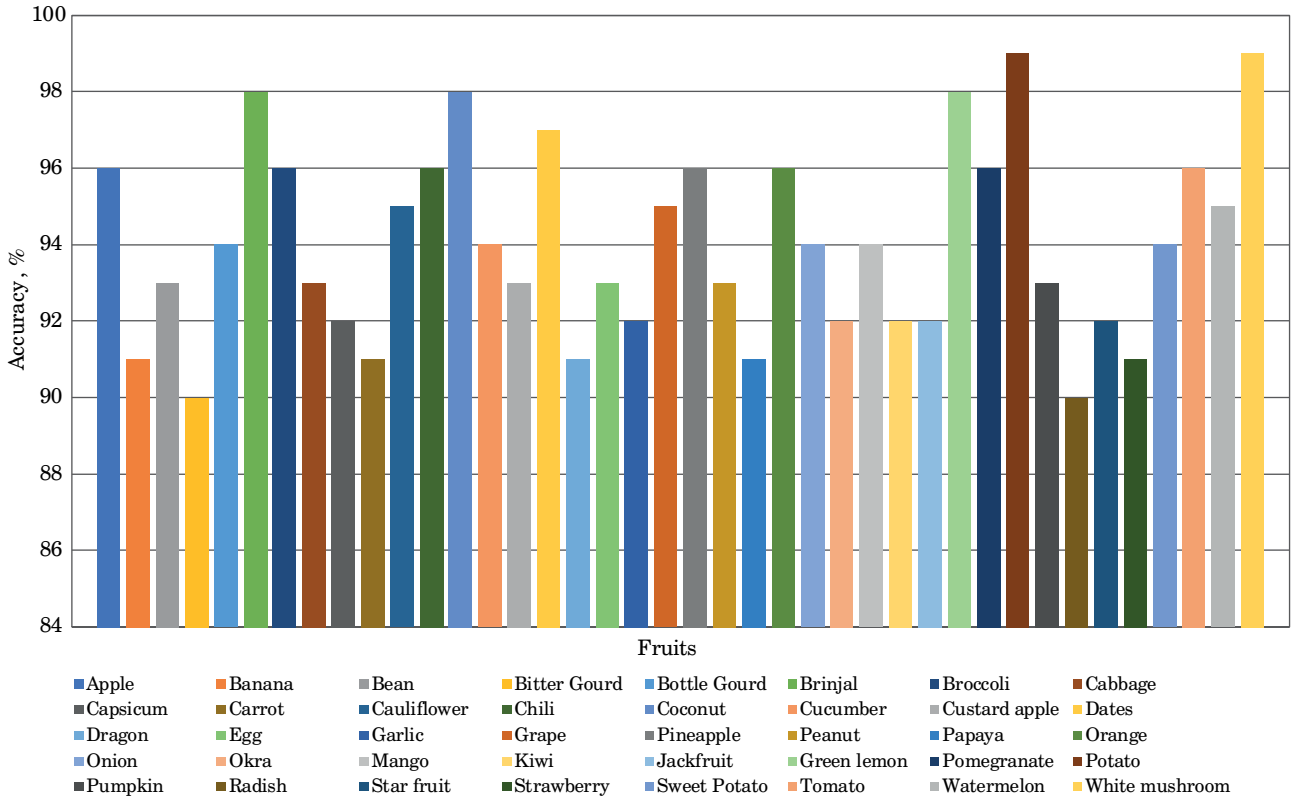
■ ***Table 2.*** Accuracy between CNN and ResNet152V2

Model	Accuracy, %
CNN	88.3
ResNet152V2	98.01

■ ***Table 3.*** Comparison of time to identify and produce results on two platforms

Platform	Time, s
Mobile	4.3
Raspberry Pi 4	2.25

enables the network to potentially exhibit superior performance during validation compared to training, as it can fully exploit its computational prowess without the hindrance of disabled neurons. Although the advanced 'Adam' optimizer may perform better on many tasks, it yields accuracy and



■ ***Fig. 9.*** Prediction accuracy of each fruit and vegetable

■ ***Fig. 10.*** Fruit and vegetable recognition result interface

recognition results that are not as close to reality for the model trained on our dataset (Table 1). Given the simplicity of the problem and the manageable size of the dataset, the 'rmsprop' optimizer yields better results and more appropriate recognition outcomes. We use the Categorical Crossentropy loss function, which is well-suited for multiclass classification problems. This approach is particularly apt for our large variety of fruits and vegetables, as it effectively prioritizes improving recognition rates for those categories with lower accuracy, and is compatible with the Softmax function [50].

During the training process, we employ callback functions such as Reduce Learning Rate, Model Checkpoint, and Early Stopping. These functions monitor the model's performance and halt training when they detect minimal or no improvement in accuracy across iterations, ensuring that only the best results are retained.

After a training process spanning approximately 20 epochs, the model achieved an accuracy of up to 98.01%. The prediction accuracy for each fruit and vegetable is illustrated in Fig. 9.

We also utilized a basic CNN model for identifying fruits and vegetables, although it yielded lower accuracy compared to ResNet152V2, as shown in Table 2. All models were trained on a P100 GPU, with the training process taking over three hours to complete. The time required by the model to identify and produce results on two different platforms is detailed in Table 3.

We also conducted extensive surveys on various types of fruits available in the market using the systems we designed. The results indicate that the majority of fruits and vegetables in the database set can be successfully identified, providing accurate results from various perspectives. Figure 10 illustrates the recognition results from the designed system.

Conclusions

Ensuring the high quality of fruit and vegetable datasets is paramount, especially for detecting real-world environmental conditions such as small targets within frames, low-light situations, blurriness, and obstructions. The ability to detect a wide variety of fruits and vegetables is also crucial in today's context. These aspects require careful attention when constructing and developing deep learning models for fruit and vegetable identification. Both the quality of the dataset and the architecture of the utilized model play pivotal roles, significantly impacting the performance of fruit and vegetable recognition systems.

In this study, we employed the ResNet152V2 model for fruit and vegetable recognition tasks, leveraging deep learning-based features. The preprocessing phase involved resizing, zooming, rotating, and shifting fruit and vegetable images to enrich and enhance the dataset's realism. Fruit and vegetable recognition achieved a peak accuracy of 98.01% across various field conditions. Furthermore, we developed a mobile application system featuring an intuitive, aesthetically pleasing, and fully functional interface. This system is supported by a stable and high-speed server infrastructure. Additionally, we engineered cost-effective, durable, compact, and portable IoT application hardware. Continuous improvements have been made to the system's database to enhance operational efficiency, accelerate data processing, and elevate accuracy levels.

Acknowledgments

Pham Cong Thang (corresponding author) would like to thank his colleagues at the Faculty of Information Technology, DUT, for their valuable feedback. The authors appreciate and are grateful to the reviewers and editors for their insightful comments and suggestions.

References

1. Aular J., Natale W. Mineral nutrition and fruit quality of some tropical fruit: guava, mango, banana, and papaya. *Revista Brasileira de Fruticultura*, 2013, no. 35, pp. 1214–1231. doi:10.1590/S0100-29452013000400033
2. Kumoro A. C., Alhanif M., Wardhani, D. A. Critical review on tropical fruits seeds as prospective sources of nutritional and bioactive compounds for functional foods development: A case of Indonesian exotic fruits. *International Journal of Food Science*, 2020, vol. 2020, pp. 1–15. doi:10.1155/2020/4051475
3. Hsouna A. B., Sadaka C., Mekinić I. G., Garzoli S., Švarc-Gajić J., Rodrigues F., Morais S., Moreira M. M., Ferreira E., Spigno G., Brezo-Borjan T., Akacha B. B., Saad R. B., Delerue-Matos C., Mnif W. The chemical variability, nutraceutical value, and food-industry and cosmetic applications of citrus plants: A critical review. *Antioxidants*, 2023, vol. 12, iss. 2, pp. 1–37. doi:10.3390/antiox12020481
4. Xiao F., Wang H., Xu Y., Zhang R. Fruit detection and recognition based on deep learning for automatic harvesting: An overview and review. *Agronomy*, 2023, vol. 13, iss. 6, pp. 1–32. doi:10.3390/agronomy13061625
5. Ukwuoma C. C., Zhiguang Q., Heyat Md B. B., Ali L., Almaspoor Z., Monday H. N. Recent advancements in fruit detection and classification using deep learning techniques: A critical review. *Mathematical Problems in Engineering*, 2022, vol. 2022, pp. 1–29. doi:10.1155/2022/9210947
6. Ismail N., Malik O. A. Real-time visual inspection system for grading fruits using computer vision and deep learning techniques. *Information Processing in Agriculture*, 2022, vol. 9, iss. 1, pp. 24–37. doi:10.1016/j.inpa.2021.01.005
7. Ray P., Pradhan S., Sharma R., Rasaily A., Swaraj A., Pradhan A. IoT based fruit quality measurement system. *Intern. Conf. on Green Engineering and Technologies (IC-GET)*, 2016, pp. 1–5. doi:10.1109/GET.2016.7916620
8. Gawas A., et al. E-fresh: Computer vision and IoT framework for fruit freshness detection. *Intern. Conf. on Advances in Computing, Communication, and Control (ICAC3)*, 2021, pp. 1–6. doi:10.1109/ICAC353642.2021.9697306
9. Behera S. K., Sethy P. K., Sahoo S. K., Panigrahi S., and Rajpoot S. C. On-tree fruit monitoring system using IoT and image analysis. *Concurrent Engineering*, 2021, vol. 29, iss. 1, pp. 6–15. doi:10.1177/1063293X20988395
10. Gupta S., Tripathi A. K. Fruit and vegetable disease detection and classification: Recent trends, challenges, and future opportunities. *Engineering Applications of Artificial Intelligence*, 2024, no. 133, pp. 1–30. doi:10.1016/j.engappai.2024.108260
11. Jana S., Basak S., Parekh R. Automatic fruit recognition from natural images using color and texture features. *Devices for Integrated Circuit (DevIC)*, 2017, pp. 620–624. doi:10.1109/DEVIC.2017.8074025
12. Lv J., Zhao D. A., Wei J., Ding S. Recognition of apple fruit in natural environment. *Optik*, 2016, vol. 127, iss. 3, pp. 1354–1362. doi:10.1016/j.ijleo.2015.10.177
13. Seng W. C., Mirisaee S. H. A new method for fruits recognition system. *Intern. Conf. on Electrical Engineering and Informatics*, 2009, pp. 130–134. doi:10.1109/ICEEI.2009.5254804
14. Shakil R. Addressing agricultural challenges: An identification of best feature selection technique for dragon fruit disease recognition. *Array*, 2023, vol. 20, 100326, pp. 1–9. doi:10.1016/j.array.2023.100326
15. Wu G., Li B., Zhu Q., Huang M., Guo Y. Using color and 3D geometry features to segment fruit point cloud and improve fruit recognition accuracy. *Computers and Electronics in Agriculture*, 2020, vol. 174, 105475, pp. 1–8. doi:10.1016/j.compag.2020.105475
16. Rachmawati E., Supriana I., Khodra M. L., Firdaus F. Integrating semantic features in fruit recognition based on perceptual color and semantic templat. *Information Processing in Agriculture*, 2022, vol. 9, iss. 2, pp. 316–334. doi:10.1016/j.inpa.2021.02.004
17. Zaki N., Singh H., Krishnan A., Alnaqbi A., Alneyadi S., Alnaqbi S., Alhindaassi S., Alam M., Eldin A. K. Transfer learning and explainable artificial intelligence enhance the classification of date fruit varieties. *International Conf. on Innovations in Information Technology (IIT)*, 2023, pp. 222–227. doi:10.1109/IIT59782.2023.10366495
18. Gill H. S., Murugesan G., Mehbodniya A., Sajja G. S., Gupta G., Bhatt A. Fruit type classification using deep learning and feature fusion. *Computers and Electronics in Agriculture*, 2020, vol. 211, 107990, pp. 1–6. doi:10.1016/j.compag.2023.107990
19. Chen J., Liu H., Zhang Y., Zhang D., Ouyang H., Chen X. A multiscale lightweight and efficient model based on YOLOv7: Applied to citrus orchard. *Plants*, 2022, vol. 11, 3260, pp. 1–17. doi:10.3390/plants11233260
20. Bai Y., Yu J., Yang S., Ning J. An improved YOLO algorithm for detecting flowers and fruits on strawberry seedlings. *Biosystems Engineering*, 2024, vol. 237, pp. 1–12. doi:10.1016/j.biosystemseng.2023.11.008
21. Qiang J., Liu W., Li X., Guan P., Du Y., Liu B., Xiao G. Detection of citrus pests in double backbone network based on single shot multibox detector. *Computers and Electronics in Agriculture*, 2023, vol. 212, 108158, pp. 1–11. doi:10.1016/j.compag.2023.108158
22. Liu W., et al. SSD: Single shot MultiBox detector. Computer vision – ECCV. *Springer International Publishing*, 2016, pp. 21–37. doi:10.1007/978-3-319-46448-0_2
23. Al-Hami M., Pietron M., Casas R., Wielgosz M. Methodologies of compressing a stable performance convolutional neural networks in image classification. *Neural Processing Letters*, 2020, vol. 51, pp. 105–127. doi:10.1007/s11063-019-10076-y

24. Jiang B., He J., Yang S., Fu H., Li T., Song H., He D. Fusion of machine vision technology and AlexNet-CNNs deep learning network for the detection of postharvest apple pesticide residues. *Artificial Intelligence in Agriculture*, 2019, vol. 1, pp. 1–8. doi:10.1016/j.aiia.2019.02.001

25. Li Z. Vegetable recognition and classification based on improved VGG deep learning network model. *International Journal of Computational Intelligence Systems*, 2020, vol. 13, iss. 1, pp. 559–564. doi:10.2991/ijcis.d.200425.001

26. Yang H., Ni J., Gao J., Han Z., Luan T. A novel method for peanut variety identification and classification by improved VGG16. *Scientific Reports*, 2021, vol. 11, pp. 1–17. doi:10.1038/s41598-021-95240-y

27. Xiang Q., Wang X., Li R., Zhang G., Lai J., Hu Q. Fruit image classification based on MobileNetV2 with transfer learning technique. *Intern. Conf. on Computer Science and Application Engineering*, 2019, pp. 1–7. doi:10.1145/3331453.3361658

28. Jain P., Chawla P., Masud M., Mahajan S., Pandit A. K. Automated identification algorithm using CNN for computer vision in smart refrigerators. *Computers, Materials and Continua*, 2022, vol. 71, no. 2, pp. 3337–3353. doi:10.32604/cmc.2022.023053

29. Yang Y., Wang L., Huang M., Zhu Q., Wang R. Polarization imaging based bruise detection of nectarine by using ResNet-18 and ghost bottleneck. *Postharvest Biology and Technology*, 2022, vol. 189, 111916, pp. 1–11. doi:10.1016/j.postharvbio.2022.111916

30. Buyukarikan B., Ulker E. Classification of physiological disorders in apples fruit using a hybrid model based on convolutional neural network and machine learning methods. *Neural Computing and Applications*, 2022, vol. 34, pp. 16973–16988. doi:10.1007/s00521-022-07350-x

31. Yao N., Ni F., Wu M., Wang H., Li G., Sung W.-K. Deep learning-based segmentation of peach diseases using convolutional neural network. *Frontiers in Plant Science*, 2022, vol. 13, pp. 1–14. doi:10.3389/fpls.2022.876357

32. Min W. Vision-based fruit recognition via multi-scale attention CNN. *Computers and Electronics in Agriculture*, 2023, vol. 210, 107911, pp. 1–11. doi:10.1016/j.compag.2023.107911

33. Hadipour-Rokni R., Askari Asli-Ardeh E., Jahanbakhshi A., Esmaili paeen-Afrakoti I., Sabzi S. Intelligent detection of citrus fruit pests using machine vision system and convolutional neural network through transfer learning technique. *Computers in Biology and Medicine*, 2023, vol. 155, 1–8. doi:10.1016/j.compbiomed.2023.106611

34. Azadnia R., Fouladi S., Jahanbakhshi A. Intelligent detection and waste control of hawthorn fruit based on ripening level using machine vision system and deep learning techniques. *Results in Engineering*, 2023, vol. 17, 100891, pp. 1–13. doi:10.1016/j.rineng.2023.100891

35. Rajak P., Ganguly A., Adhikary S., Bhattacharya S. Internet of things and smart sensors in agriculture: Scopes and challenges. *Journal of Agriculture and Food Research*, 2023, vol. 14, pp. 1–13. doi:10.1016/j.jafr.2023.100776

36. Kasera R. K., Gour S., Acharjee T. A comprehensive survey on IoT and AI based applications in different pre-harvest, during-harvest and post-harvest activities of smart agriculture. *Computers and Electronics in Agriculture*, 2024, vol. 216, pp. 1–24. doi:10.1016/j.compag.2023.108522

37. Wason R., Choudhary P., Tomar A., Arora D. A novel, low-cost, smart IoT based framework for fruit and vegetable quality detection during transit in India. *International Journal of Information Technology*, 2023, vol. 15, pp. 1509–1519. doi:10.1007/s41870-023-01177-y

38. Nirale P., Madankar M. Design of an IoT based ensemble machine learning model for fruit classification and quality detection. *Intern. Conf. on Emerging Trends in Engineering and Technology – Signal and Information Processing*, 2022, pp. 1–6. doi:10.1109/ICETET-SIP-2254415.2022.9791718

39. Rebelo R. M. L., Pereira S. C. F., Queiroz M. M. The interplay between the Internet of things and supply chain management: Challenges and opportunities based on a systematic literature review. *Benchmarking: An International Journal*, 2022, vol. 29, iss. 2, pp. 683–711. doi:10.1108/BIJ-02-2021-0085

40. Taj S., Imran A. S., Kastrati Z., Daudpota S. M., Memon R. A., Ahmed J. IoT-based supply chain management: A systematic literature review. *Internet of Things*, 2023, vol. 24, 100982, pp. 1–25. doi:10.1016/j.iot.2023.100982

41. Mishra S., Khatri S. K., Johri P. IoT based automated quality assessment for fruits and vegetables using infrared. *Intern. Conf. on Information Systems and Computer Networks (ISCON)*, 2019, pp. 134–138. doi:10.1109/ISCON47742.2019.9036165

42. Putra B. T. W., Indracahyana K. S., Fanshuri B. A. Development of a handheld IoT-based fruit harvester to support agrotourism. *Microprocessors and Microsystems*, 2022, vol. 91, pp. 1–7. doi:10.1016/j.micpro.2022.104550

43. Kavitha R., Shanthi T., Maithili P., Roopika J., Naveen Kumar K., Saravanakumar K. Deep learning and Internet of Things based detection of diseases and prediction of pesticides in fruits. *Intern. Conf. on Trends in Electronics and Informatics (ICOEI)*, 2023, pp. 1133–1140. doi:10.1109/ICOEI56765.2023.10125946

44. Nasir I. M., Bibi A., Shah J. H., Khan M. A., Sharif M., Iqbal K., Nam Y., Kadry S. Deep learning-based classification of fruit diseases: An application for precision agriculture. *Computers, Materials & Continua*, 2021, vol. 66, no. 2, pp. 1949–1962. doi:10.32604/cmc.2020.012945

45. Hayajneh A. M., Batayneh S., Alzoubi E., Alwedyan M. TinyML olive fruit variety classification by means of

convolutional neural networks on IoT Edge devices. *AgriEngineering*, 2023, vol. 5, iss. 4, pp. 2266–2283. doi:10.3390/agriengineering5040139

46. Augustin A., Kiliroor C. C. (2024) IoT-based pesticide detection in fruits and vegetables using hyperspectral imaging and deep learning. *Cognitive Computing and Cyber Physical Systems, Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*, Springer, Cham, 2023, vol. 536, pp. 74–83. doi:10.1007/978-3-031-48888-7_6

47. He K., Zhang X., Ren S., Sun J. *Identity Mappings in Deep Residual Networks*. In: *Computer Vision — ECCV 2016. ECCV 2016*. Lecture Notes in Computer Science, 2016, vol. 9908, pp. 630–645. doi:10.1007/978-3-319-46493-0_38

48. *React Native*. Available at: https://reactnative.dev (accessed 30 January 2024).

49. *Raspberry Pi 4*. Available at: https://www.raspberrypi.org/products/raspberry-pi-4-model-b (accessed 30 January 2024).

50. Murphy K. P. *Probabilistic Machine Learning: An Introduction. Adaptive Computation and Machine Learning series*. The MIT Press, 2020. 864 p.

УДК 004.9
doi:10.31799/1684-8853-2024-2-9-20
EDN: XSSHJI

Система интернета вещей на основе глубокого обучения для распознавания фруктов и овощей

Фам Конг Тханг[а], PhD, преподаватель, orcid.org/0000-0002-6428-102X, pcthang@dut.udn.vn
Нгуен Ван Зунг[а], студент, orcid.org/0009-0004-1282-184X
Ле Туан Нгуен Хой[а], студент, orcid.org/0009-0001-1191-2502
Фам Зуи Тин[а], студент, orcid.org/0009-0002-2314-1503
Чан Тхи Тху Тхао[б], магистр, преподаватель, orcid.org/0000-0001-7705-2405
[а]Университет Дананга — Университет науки и техники, Нгуен Лыонг Банг, 54, Дананг, 550000, Вьетнам
[б]Университет Дананга — Университет экономики, Нгу Хань Шон, 71, Дананг, 550000, Вьетнам

Введение: в контексте растущей важности овощей и фруктов как значимых источников питания возрастает спрос на передовую технологию их распознавания на основе компьютерного зрения в цепочке поставок. Эта технология имеет решающее значение на различных этапах, включая сбор урожая, сортировку и контроль качества. **Цель:** разработать передовые системы распознавания фруктов путем интеграции устройств интернета вещей, таких как камеры и датчики, с алгоритмами глубокого обучения. **Результаты:** использованы сверточные нейронные сети для усовершенствования возможностей распознавания фруктов путем извлечения сложных особенностей изображений, для чего изображения овощей и фруктов загружались в предварительно обученные модели глубокого обучения. Среди этих моделей ResNet152V2 отличается устойчивостью к шуму и искажениям, что делает ее подходящей для реальных приложений. Ее масштабируемость позволяет ей обрабатывать большие наборы данных и более сложные задачи, постоянно достигая высокой точности распознавания изображений даже в сложных условиях. Набор данных, полученный из онлайн-каналов и полевых каналов, включал около 31 000 изображений фруктов и овощей. В процессе обучения использовались такие методы, как GlobalAveragePooling2D, полностью связанные слои, отсев для предотвращения переобучения и активация softmax, что привело к впечатляющей точности 98,01 % для ResNet152V2 после 20 эпох по сравнению с производительностью базовой модели сверточной нейронной сети 88,3 %. Примечательно, что при развертывании на мобильных платформах и Raspberry Pi 4 время идентификации составило 4,3 и 2,25 с соответственно. Одновременно разработано прикладное программное обеспечение и аппаратная система интернета вещей для мониторинга и улучшения процесса распознавания фруктов и овощей. **Практическая значимость:** решена проблема распознавания фруктов и овощей с помощью модели глубокого обучения ResNet152V2 и набора данных. Достигнуты высокая точность и быстрое прогнозирование, разработано экономичное и надежное оборудование для приложений интернета вещей.

Ключевые слова — распознавание фруктов и овощей, глубокое обучение, машинное обучение, ResNet152V2.

Для цитирования: Pham C. T., Nguyen V. D., Le T. N. K., Pham D. T., Tran T. T. T. Deep learning-based IoT system for fruit and vegetable recognition. *Информационно-управляющие системы*, 2024, № 2, с. 9–20. doi:10.31799/1684-8853-2024-2-9-20, EDN: XSSHJI

For citation: Pham C. T., Nguyen V. D., Le T. N. K., Pham D. T., Tran T. T. T. Deep learning-based IoT system for fruit and vegetable recognition. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2024, no. 2, pp. 9–20. doi:10.31799/1684-8853-2024-2-9-20, EDN: XSSHJI

УДК 004.93'1
doi:10.31799/1684-8853-2024-2-21-38
EDN: YIVAYM

Научные статьи
Articles

Аутентификация по голосовым паролям с обеспечением конфиденциальности биометрических данных на основе корреляционных нейронов

А. Е. Сулавко[а], *канд. техн. наук, доцент, orcid.org/0000-0002-9029-8028, sulavich@mail.ru*
Д. П. Иниватов[а], *ассистент, orcid.org/0000-0001-9911-1218*
В. И. Васильев[б], *доктор техн. наук, профессор, orcid.org/0000-0002-6105-5481*
П. С. Ложников[а], *доктор техн. наук, профессор, orcid.org/0000-0001-7878-1976*
[а]*Омский государственный технический университет, Мира пр., 11, Омск, 644050, РФ*
[б]*Уфимский университет науки и технологий, Заки Валиди ул., 32, Уфа, 450076, РФ*

Введение: *вопрос защиты биометрических данных от компрометации тесно связан с вопросами производительности. Существующие методы биометрической аутентификации по голосу либо не позволяют защитить голосовые данные от компрометации, либо дают высокий процент ошибочных решений и, кроме того, не гарантируют устойчивость к дрейфу голосовых образов.* ***Цель:*** *разработать метод биометрической аутентификации по голосу, устойчивый к дрейфу биометрических данных, с обеспечением конфиденциальности параметров голоса.* ***Результаты:*** *предложен метод аутентификации с использованием нейросетевых преобразователей биометрия-код на базе модифицированной модели корреляционных нейронов и алгоритмов их обучения. Вычислительный эксперимент показал, что корреляционные связи между признаками содержат информацию об образах, которая не дублирует информацию, содержащуюся в признаках. Преобразователь биометрия-код на базе корреляционных нейронов дает гораздо меньший процент ошибок и в разы большую длину ключа, чем классическая модель на базе алгоритма обучения ГОСТ Р 52633.5. Количество ошибок составило 3,26 %. При изменении состояния субъекта (опьянении или сонном состоянии) для разработанного метода количество ошибок повышается не столь существенно, чем для классической модели нейросетевого преобразователя биометрия-код.* ***Практическая значимость:*** *результаты могут использоваться для повышения защищенности компьютерных ресурсов от неавторизованного доступа и биометрических данных от компрометации.* ***Обсуждение:*** *объединение нейронов различного типа в единый слой позволит создать более устойчивые и надежные нейросетевые преобразователи биометрия-код.*

Ключевые слова *— защищенное исполнение нейросетевых алгоритмов, обработка коррелированных биометрических признаков, голосовая биометрия, нейросетевые преобразователи биометрия-код, анализ временных рядов, автокодировщики.*

Для цитирования: Сулавко А. Е., Иниватов Д. П., Васильев В. И., Ложников П. С. Аутентификация по голосовым паролям с обеспечением конфиденциальности биометрических данных на основе корреляционных нейронов. *Информационно-управляющие системы*, 2024, № 2, с. 21–38. doi:10.31799/1684-8853-2024-2-21-38, EDN: YIVAYM
For citation: Sulavko A. E., Inivatov D. P., Vasilyev V. I., Lozhnikov P. S. Authentication based on voice passwords with the biometric template protection using correlation neurons. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2024, no. 2, pp. 21–38 (In Russian). doi:10.31799/1684-8853-2024-2-21-38, EDN: YIVAYM

Введение

Сегодня мировой рынок биометрии проходит фазу активного роста (по данным MarketsandMarkets, к 2025 г. его объем составит 68 млрд долл.). Биометрические системы внедряются повсеместно: на объектах критической информационной инфраструктуры, в банковской сфере, государственном секторе (более 80 стран используют биометрические паспорта), в сфере управления транспортом и городом. Рост рынка биометрических систем обусловлен новыми тенденциями и вызовами, с которыми столкнулись общество и государство:

— увеличением объемов данных о действиях пользователей в сети Интернет, которые могут быть использованы в злоумышленных целях (обострились проблемы приватности, анонимности пользователей и защищенности биометрических шаблонов от компрометации);

— применением технологий искусственного интеллекта (ИИ) для реализации хакерских атак, дезинформации, мошенничества, фальсификации биометрических образов человека (например, при помощи deepfake, голосовых синтезаторов);

— заменой традиционных биометрических образов отпечатка пальца на более удобные образы голоса, лица и др., пригодные для бесконтактной аутентификации, но в большей степени подверженные дрейфу (изменчивости).

В связи с этим современная высоконадежная биометрическая система должна строиться на основе доверенного ИИ, устойчивого к деструктивным факторам (дрейфу биометрических данных, компьютерным атакам). В России системы вы-

соконадежной биометрической аутентификации строятся на базе специальных архитектур ИИ — нейросетевых преобразователей биометрия-код (НПБК), которые позволяют связать биометрический образ субъекта с его криптографическим ключом или паролем [1].

Одной из перспективных биометрических модальностей является голос. Данный тип образов вместе с изображением лица используется в единой биометрической системе в соответствии с Федеральным законом № 572. Однако голосовые образы уязвимы с точки зрения компрометации, поэтому в ответственных приложениях лучше использовать не открытый голосовой образ (как при текстонезависимом распознавании диктора), а тайный образ — пароль, который произносится при аутентификации.

Настоящее исследование посвящено разработке метода биометрической аутентификации по голосу с обеспечением защищенности данных голоса от компрометации и устойчивости к их дрейфу. Работа является продолжением исследований [1], так как за основу предлагаемого метода взята модель НПБК на базе корреляционных нейронов (анализирующих корреляцию между признаками), которая изначально была предложена для аутентификации по внутреннему строению уха.

Краткий анализ проблемы и достигнутых результатов

В мировой практике сложилось несколько подходов к повышению надежности биометрических систем аутентификации с обеспечением конфиденциальности биометрических данных, которые основаны на использовании нечетких экстракторов, отменяемой биометрии, искусственных нейронных сетей или шифровании, в том числе гомоморфном. Проблемы гомоморфного шифрования заключаются в склонности гомоморфных шифров к накоплению ошибок (чем больше математических операций произведено с гомоморфным шифртекстом, тем больше вероятность некорректного результата этих операций [2], а также низкой производительности. В подтверждение этому факту приведем несколько работ. В исследовании [3] применяются полное гомоморфное шифрование биометрических образов и параллельные вычисления. Авторы отмечают, что процедура распознавания личности обладает низким быстродействием. Разработана [4] модель защиты мультимодальных биометрических шаблонов на базе гомоморфного шифрования по стандарту ISO/IEC 24745:2011. Основной недостаток модели также заключается в низкой скорости. В работе [5] предлагается протокол аутентификации на основе радужки с использованием гомоморфного шифрования. Среди недостатков разработанного решения можно отметить низкую производительность.

Отменяемая биометрия позволяет хранить не исходные образы субъектов, а их шаблоны, искаженные при помощи необратимых функций. Восстановить изначальные образы из сохраненного шаблона не представляется возможным. В исследовании [6] реализован облачный сервис, в котором биометрические шаблоны защищены методом случайных проекций (точность биометрической аутентификации по параметрам радужки составила 99,55 %). В статье [7] авторы достигли коэффициента равной вероятности ошибок EER = 0,2 % (Equal Error Rate), представив систему аутентификации по лицу и отпечатку пальца с шифрованием шаблонов, основанную на применении эволюционного генетического алгоритма.

Работа нечетких экстракторов (fuzzy vault, fuzzy extractor, fuzzy commitment, fuzzy embedder) обусловлена слабыми решающими правилами — неспособностью анализировать данные подобно нейронным сетям, и в случае с недостаточно информативными признаками экстракторы демонстрируют относительно низкую эффективность в задаче обработки рукописных образов (доля ошибок «ложного допуска» FAR = 0,2 % (False Acceptance Rate) при доле ошибок «ложного отказа» FRR = 76,53 % (False Rejection Rate), а также FAR = 6,91 % при FRR = 7,85 %) [8]. Применение схемы fuzzy vault к векторам извлеченных из изображений лиц с использованием методов квантования и бинаризации признаков исследуется в работе [9]. Ученые достигли показателей FAR = 1 % при FRR = 0,1 %.

На данный момент действует ряд международных стандартов, связанных с вопросами защиты биометрических систем от компьютерных атак (ISO/IEC 19792:2009, ISO/IEC 24761:2019, ISO/IEC 24745:2022, ISO/IEC 30107). Но эти стандарты не позволяют устранить ряд актуальных угроз (извлечение знаний моделей ИИ, компрометацию открытых биометрических образов, состязательные атаки). В России действует серия национальных ГОСТ Р 52633, не имеющих международных аналогов. Эти ГОСТы регламентируют особенности разработки, обучения и тестирования систем высоконадежной биометрической аутентификации, которые должны строиться на базе НПБК, позволяющих связать криптографический ключ или пароль пользователя с его биометрическим образом. НПБК не имеют недостатков, характерных для нечетких экстракторов [10], и значительно их превосходят, так как дают большую длину ключа при

меньших значениях FRR и FAR [11]. Технически НПБК позволяют связать биометрический образ с ключом любой длины. Однако определенные ограничения все-таки существуют.

Первое из них не позволяет использовать каждый биометрический признак дважды при нейросетевой обработке (входы нейронов в НПБК не могут дублироваться), иначе НПБК становятся подверженными атаке Маршалко [12], основанной на наблюдении одинаковых весовых коэффициентов в таблицах нейросетевых функционалов. С учетом этого требования длина ключа для НПБК будет снижена. Например, для технологии аутентификации в защищенном режиме по рукописной подписи при наличии 416 признаков, извлекаемых из рукописных образов, может получиться 26 нейронов, у которых имеется по 16 неповторяющихся входов [13]. Длина ключа 26 бит явно недостаточна для практических целей. Аналогично дело обстоит и с голосовыми образами (при том же количестве входов с учетом соблюдения данного требования при количестве признаков от 521 до 728 [14] мы получим длину ключа от 32 до 49 бит).

Второе ограничение связано с возможностью проведения атаки «извлечения знаний» из обученного НПБК путем статистического анализа стабильности выходов ПБК при поступлении на его входы естественных и синтетических образов «Чужих». В работах [10, 11] описываются результаты исследования НПБК, в том числе касающиеся энтропии их откликов при поступлении на вход образов «Чужих». Для защиты от атаки «извлечения знаний» можно применить действенный метод криптографической защиты. Нейроны выстраиваются в цепочку, и после обучения НПБК параметры каждого нейрона шифруются на ключе, зависящем от выходов всех предыдущих нейронов в цепочке [10, 11]. Тем не менее известны другие варианты атак на классические НПБК [15], которые могут работать даже при реализации криптографической защиты. Атакам подвержены нейроны с бинарными выходами (когда каждый нейрон на выходе дает один бит), которые являются «узким местом».

Наконец, одной из ключевых проблем машинного обучения и классических НПБК в частности является проблема концептуального дрейфа — изменения взаимосвязи между данными и прогнозируемым явлением, которое не было учтено при обучении модели ИИ. Если дрейф данных (сбои датчиков, изменение единиц измерения) часто устраняется относительно легко (следует продумать все возможные изменения, которые могут быть спрогнозированы при обучении модели), то концептуальный дрейф устранить затруднительно, так как нельзя заранее знать, как в будущем изменится прогнозируемое явление.

В биометрии дрейф модели можно условно разделить на две категории:

— кратковременный (голос меняется при опьянении субъекта или заболевании горла) [16];

— долговременный (медленные и, как правило, необратимые со временем изменения биометрического образа пользователя).

Несмотря на различные причины дрейфа, оба типа изменений крайне сложно спрогнозировать. Если для статических биометрических образов (отпечатка пальца, радужки, сетчатки, лица) дрейф появляется только при физических нарушениях, таких как травма, порезы и т. д., то для динамических биометрических образов этих изменений почти невозможно избежать (например, голос меняется в зависимости от эмоционального состояния).

Можно сформулировать несколько общих приемов и подходов, предназначенных для снижения негативного влияния дрейфа. Например, периодическое обновление модели дает положительный эффект, если есть данные для переобучения. При этом может применяться взвешивание данных — присвоение большего веса наиболее актуальным обучающим примерам и меньшего веса данным, полученным давно. Для своевременного обнаружения дрейфа используются метрики, вычисляющие статистические характеристики данных с учетом ретроспективы [17, 18], а также ансамблевые методы классификации. Однако эти методы дают ограниченный эффект. Наиболее эффективным подходом является онлайн-обучение (обучение или дообучение в процессе функционирования), которое позволяет снизить влияние концептуального дрейфа. Однако классический НПБК не может работать в режиме онлайн-обучения (весовые коэффициенты НПБК не могут быть скорректированы путем извлечения из них и устранения информации, потерявшей актуальность).

В настоящем исследовании мы пошли иным путем, используя модель нейрона, которая сама по себе, как оказалось, обладает некоторой устойчивостью к дрейфу голосовых данных.

Наборы голосовых данных для проведения экспериментов

Существующие наборы данных, которые возможно использовать для тестирования методов биометрической голосовой аутентификации, не учитывают психоэмоционального состояния диктора (VoxCeleb, TIMIT, RedDots, Common Voice, VoxForge, LibriSpeech, NIST SRE). Кроме того, большая часть этих наборов данных применима для систем текстонезависимого распозна-

вания личности диктора. Наиболее актуальной на сегодня базой голосовых паролей, используемой для оценки современных методов текстозависимой классификации дикторов, является RedDots [19]. Набор данных включает голоса 100 испытуемых, речь которых записывалась еженедельно в течение года. Каждый доброволец произносил 24 предложения на каждой сессии, включая 22 повторяющихся и два свободных текстовых. Всего в наборе данных 124 800 записей. Корпус создан для исследования влияния феномена «старения» на распознавание голоса. Данная база использовалась в настоящем исследовании для тестирования предлагаемой модели.

Психоэмоциональное (психофизиологическое) состояние субъекта является одним из ключевых факторов, вызывающих дрейф [16]. Поэтому был сформирован собственный набор данных, учитывающий следующие состояния испытуемых: нормальное (спокойное), возбужденное, сонное и алкогольного опьянения. Набор данных можно разделить на две части.

1. «Зарегистрированные субъекты» («Все Свои»): 65 дикторов, каждый воспроизвел образ определенного голосового пароля не менее 80 раз, данные собраны в три этапа с интервалом несколько недель:

— на 1-м этапе каждый испытуемый ввел не менее 40 примеров, при этом испытуемые пребывали в нормальном состоянии (выспались перед экспериментом и не подвергались никаким воздействиям);

— на 2-м этапе каждый испытуемый ввел 20 примеров в сонном состоянии после приема седативных средств;

— на 3-м этапе каждый испытуемый ввел 20 примеров в состоянии легкого алкогольного опьянения, при котором концентрация алкоголя в крови составляет от 0,5 до 1 ‰ (согласно рекомендациям Минздрава, в данном состоянии речь субъекта становится менее разборчивой), количество алкоголя для получения данной стадии опьянения рассчитывалось по формуле Видмарка исходя из пола и веса субъекта [16].

Примеры, полученные на этапе 1, могут целиком или частично использоваться для обучения системы, в том числе в составе валидационной выборки (в настоящей работе для обучения использовано по 20 примеров, остальные — для тестирования, валидационная выборка при обучении НПБК не применяется). Примеры, полученные на этапах 2 и 3, рекомендуется использовать только для тестирования.

2. «Неизвестные Чужие»: 650 примеров других голосовых образов (фраз, паролей), воспроизведенных другими субъектами, не вошедшими в базу «Зарегистрированные субъекты». Данная выборка должна использоваться только в целях тестирования.

Для записи использовался микрофон Fifine K680 (чувствительность 34 дБ, диапазон частот 20÷20 000 Гц, соотношение сигнал/шум 78 дБ). Запись производилась в тихом помещении при отсутствии внешних источников шума.

Звуковые сигналы имеют следующие параметры: размер семпла $\Psi = 16$ бит, частота дискретизации $\Omega = 16$ кГц. Сформированный набор данных применялся для обучения и тестирования НПБК. Открытые наборы данных VoxCeleb и TIMIT использовались для предварительного обучения нейронных сетей, извлекающих признаки из голосового образа перед подачей образа в НПБК.

Архитектурные принципы построения метода аутентификации субъектов по голосу на базе НПБК

Для реализации концепции защищенного исполнения нейросетевых алгоритмов ИИ в задачах классификации образов предлагается разделить функционал ИИ на блок выделения признаков и НПБК. Блок извлечения признаков преобразует образ в вектор фиксированной длины (эту операцию можно назвать ортогонализацией образа). На этапе извлечения признаков образ нормируется, и из него удаляется незначимая информация. Блок извлечения признаков может быть реализован на основе практически любых подходов (нейронных сетей, классических методов спектрального и корреляционного анализа и др.). В общем случае блок извлечения признаков является зависимым от предметной области, так как для разных приложений входные данные могут кардинально отличаться, как и характер извлекаемой из образа информации (вектора признаков). Для обработки звука часто используются методы x-vector, d-vector, i-vector, быстрое преобразование Фурье, вычисление мел-кепстральных коэффициентов или вейвлет-преобразование. Разные подходы могут комбинироваться. В настоящей работе блок извлечения признаков строится на базе автокодировщиков.

Обучение автокодировщика [20] гипотетически может вестись алгоритмом градиентного спуска или его модификациями. Для синтеза и обучения НПБК в автоматическом режиме требуется отдельный робастной алгоритм.

Вектор признаков, извлеченный автокодировщиками, поступает на вход НПБК. Обучение НПБК должно быть автоматическим и робастным.

Извлечение признаков

Предобработка данных голосовых образов

Прежде всего голосовые образы были преобразованы в спектрограммы. Чтобы выделить из акустических образов полезную информацию и снизить дисперсию случайных выбросов при разложении сигнала в ряды Фурье, спектрограммы были преобразованы в усредненный по всем окнам (по всем временным промежуткам) амплитудный спектр (путем интегрирования спектрограмм). В настоящем исследовании использовались следующие параметры быстрого оконного преобразования Фурье: размер окна W_{size} = 4096 (четверть секунды), шаг W_{step} = 256. Длина усредненного спектра 2048 амплитуд.

Архитектуры автокодировщиков и их обучение

В голосовой биометрии часто используются методы извлечения так называемых мелкепстральных коэффициентов, а также x-, d- и i-векторов. Весомая часть исследований посвящена сравнению данных методов, что привело к выводу, что i-vector позволяет создавать менее ресурсоемкие системы, в то время как x-vector обеспечивает более высокую эффективность благодаря глубокому анализу: 5,71 % против 9,23 % EER при использовании вероятностного линейного дискриминантного анализа в качестве классификатора [21].

Альтернативным направлением является применение автокодировщиков. Можно применить сразу несколько схожих архитектур, обученных на одних и тех же данных, что позволит получить множество признаков с сильной взаимной корреляцией, необходимых для построения НПБК на базе корреляционных нейронов. По этой причине для извлечения признаков решено использовать две схожие архитектуры автокодировщиков (рис. 1). Ожидаемо, что признаки, извлекаемые автокодировщиками со схожими архитектурами, обученными на одной и той же выборке, будут в большей степени коррелированы.

При обучении применялся подход из работы [1]. Мы взяли речевые сигналы из наборов данных TIMIT и VoxCeleb1 (наборы данных имеют одинаковые параметры голосовых сигналов Ψ = 16 бит, Ω = 16 кГц [22]) с длительностью, соответствующей короткому голосовому паролю. Далее была выполнена аугментация данных [23] — образы преобразовывались в четыре представления, каждое из которых — это усредненный спектр, полученный при помощи одного из четырех типов окон (прямоугольного, Блэкмана, Барлетта, Хэмминга). Общее количество образов превысило 285 000 после аугментации. Автокодировщики обучены оптимизатором Adam (20 эпох).

При извлечении признаков также использованы две вариации образа — на базе прямоугольной оконной функции Фурье и оконной функции Хэмминга. Этот прием также применялся для получения большего числа сильно коррелированных признаков. Ожидаемо, что усредненные спектры, полученные с использованием различных типов окон, после обработки кодировщиком дадут коррелированные векторы признаков, но все-таки имеющие отличия. Чем больше коррелированных пар признаков, тем выше эффективность НПБК на базе корреляционных нейронов [1].

Математические основы используемой модели НПБК

Искривление пространства признаков

Для расчета расстояния в искривленном пространстве признаков может применяться мера Минковского

$$y = \sqrt[g]{\sum_{j=1}^{n}\left|\frac{(m_j - a_j)}{\sigma_j}\right|^g},$$

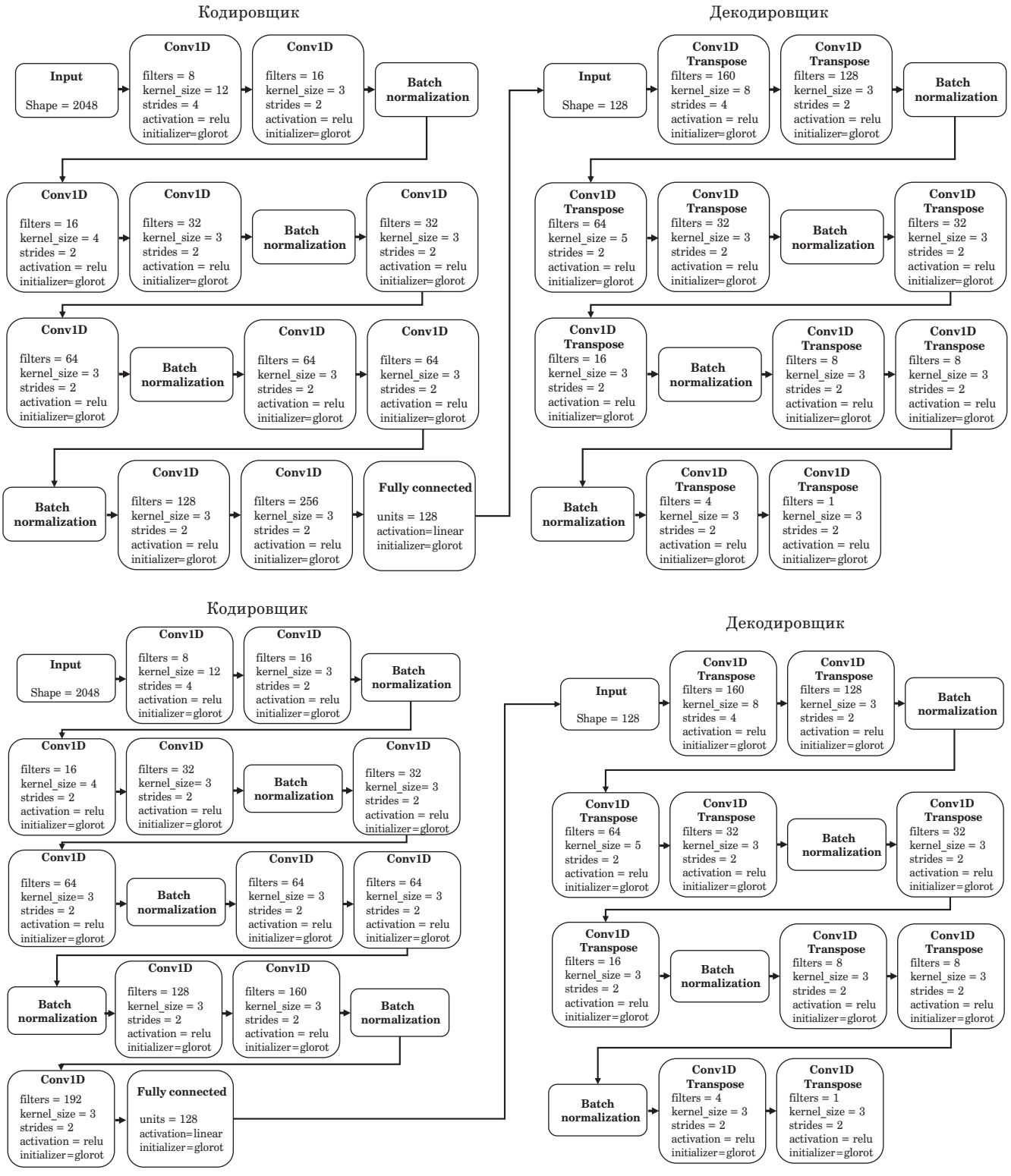
где g — степенной коэффициент; n — число признаков; m_j и σ_j — математическое ожидание и стандартное отклонение j-го признака для класса «Свой» (класс зарегистрированного пользователя); a_j — значение j-го признака.

Искривление признакового пространства возникает из-за корреляции между признаками (рис. 2). Относительно различных классов пространство признаков искривлено по-разному, так как биометрический образ каждого человека имеет уникальную матрицу коэффициентов корреляции

$$C_{j,t} = \frac{\sum_{k=1}^{K_G}(a_{t,k} - m_t)(a_{j,k} - m_j)}{\sqrt{\sum_{k=1}^{K_G}(a_{t,k} - m_t)^2 \sum_{k=1}^{K_G}(a_{j,k} - m_j)^2}}, \quad (1)$$

где K_G — количество обучающих примеров образа «Свой» (далее K_I — количество обучающих примеров образа «Чужие»); k — порядковый номер примера в обучающей выборке. На рис. 2 для класса 2 расстояние «*а*» на самом деле должно быть больше, чем расстояние «*б*», так как пространство признаков является не плоским, а искривленным.

Важным показателем j-го признака также является уровень его информативности, который

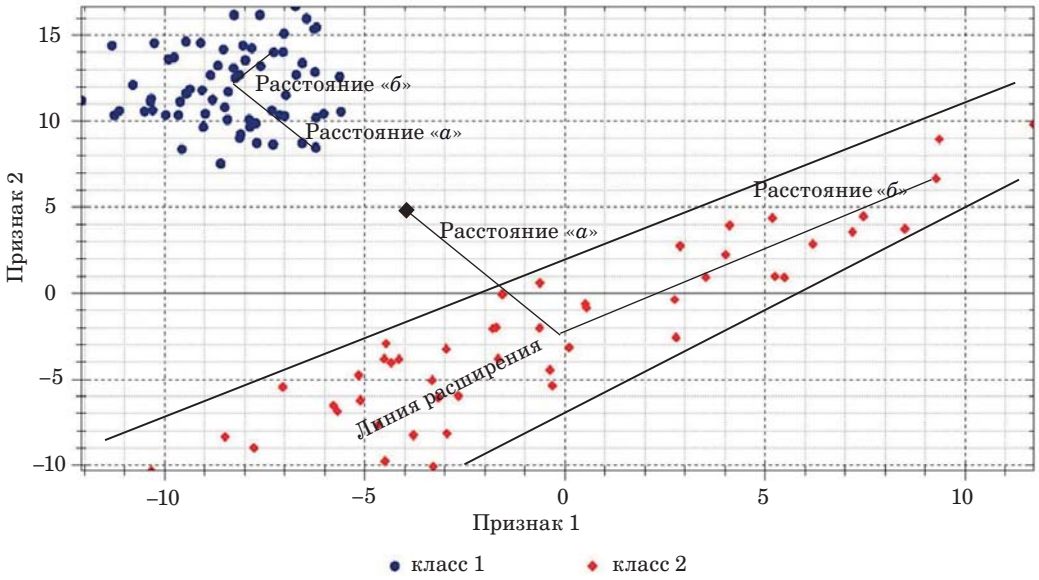


■ ***Рис. 1.*** Архитектуры использованных автокодировщиков
■ ***Fig. 1.*** Architectures of the used autoencoders

определяется количеством собственной информации для определенного класса образов [1]:

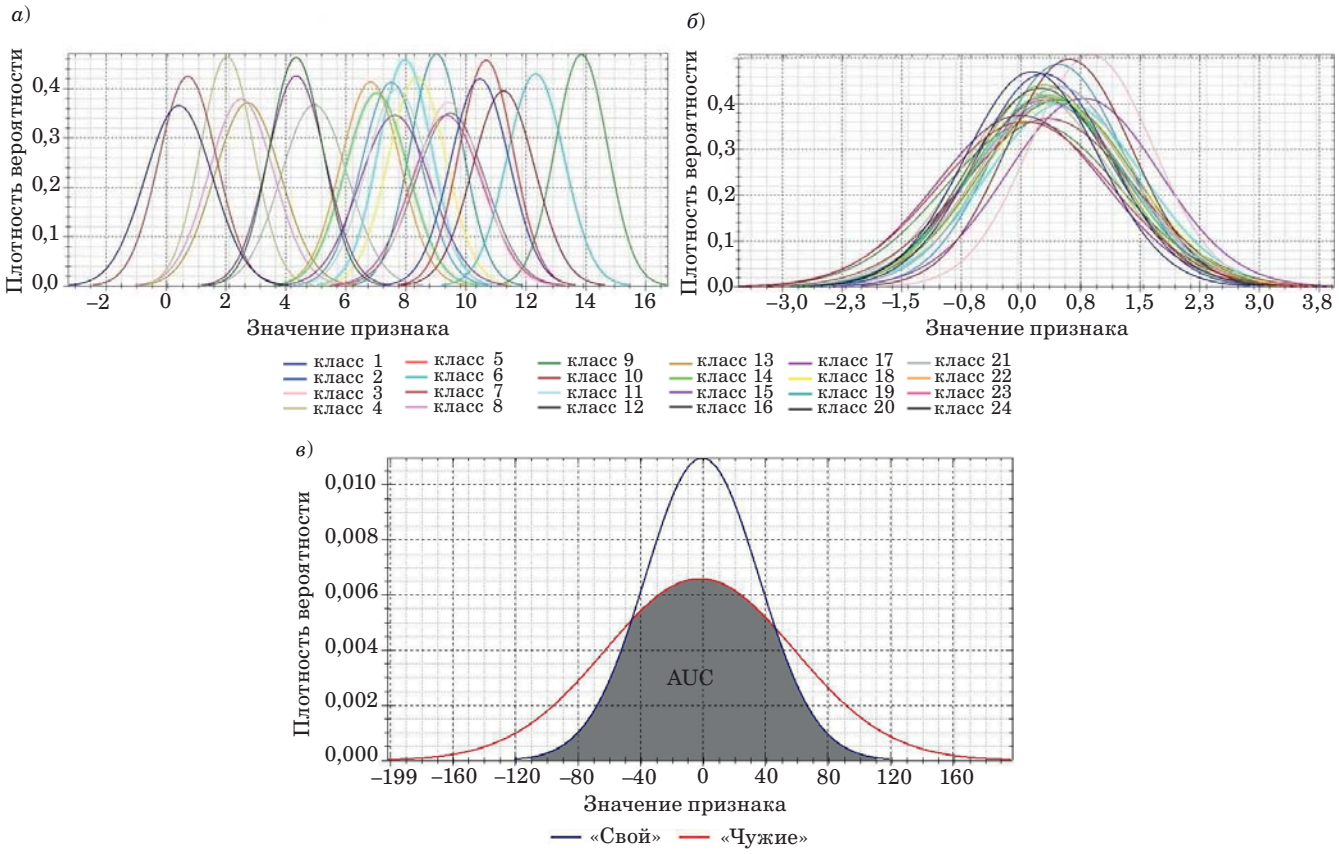
$$I_j = -\log_2(AUC(\Phi_G(a_j), \Phi_I(a_j))), \qquad (2)$$

где AUC – площадь, ограниченная функциями плотности вероятности (ФПВ) «Свой» $\Phi_G(a_j)$ и «Чужие» $\Phi_I(a_j)$, а также осью абсцисс (рис. 3, *а–в*). $\Phi_G(a_j)$ характеризует значения при-



■ ***Рис. 2.*** Пространство признаков является «плоским» относительно класса 1 (признаки независимы) и искривленным относительно класса 2 (признаки положительно коррелированы), черная точка — это образ «Чужого»

■ ***Fig. 2.*** The feature space is “flat” relative to class 1 (features are independent) and curved relative to class 2 (features are positively correlated), the black dot is the “Imposter” image



■ ***Рис. 3.*** Примеры ФПВ признака: *а*, *б* — 24 классов «Свой» ($I_{bit} \approx 1{,}75$; $I_{bit} \approx 0{,}15$ соответственно); *в* — расчет AUC через построение ФПВ «Свой» и «Чужие» [1]

■ ***Fig. 3.*** Examples of the probability density function of a feature: *a*, *б* — 24 «Genuine» classes ($I_{bit} \approx 1{,}75$; $I_{bit} \approx 0{,}15$ respectively); *в* — calculating AUC by constructing the probability density function «Genuine» and «Imposters» [1]

знака для определенного субъекта, $\Phi_I(a_j)$ характеризует значения этого же признака для всех субъектов в целом [1].

Изменяя параметр g, можно добиться снижения количества ошибок классификации. Чтобы это продемонстрировать, в настоящем исследовании проведен вычислительный эксперимент по распознаванию образов в пространстве 200 абстрактных (имитированных) признаков. Все признаки имели нормальное распределение значений (наиболее распространенный случай для биометрии). На каждом этапе эксперимента генерировалось два пространства признаков — независимых ($C \approx 0$) и зависимых ($C > 0$). Отличия этапов заключались в информативности и уровне коррелированности зависимых признаков (см. рис. 3): $I \approx 0{,}15$ при $C \approx 0$; $I \approx 0{,}15$ при $C \approx 0{,}9$; $I \approx 1{,}75$ при $C \approx 0{,}1$; $I \approx 1{,}75$ при $C \approx 0$.

Генерируемые классы образов отличались между собой параметрами распределения признаков. Значения независимых признаков генерировались методом Монте-Карло под соответствующие параметры классов. Для классов с зависимыми признаками перед формированием соответствующих образов $\bar{a}$ значения каждого признака внутри класса были отсортированы по возрастанию. Таким образом, в эксперименте смоделировано четыре варианта пространства признаков (зависимых и коррелированных с учетом двух уровней информативности). Для каждого случая сгенерировано 500 классов по 125 примеров образа на класс. Каждый классификатор обучался на 25 случайных сгенерированных примерах, остальные 100 примеров использовались для тестирования. Исходя из порогового значения для меры Минковского, принималось решение об отнесении данных к категории «Свой» или «Чужие». По окончании сессии рассчитывался показатель EER. Обобщенные результаты эксперимента показаны на рис. 4, *а–в* (все вероятности ошибок представлены в логарифмической шкале).

Мера Минковского позволяет точнее определять расстояния в искривленном пространстве признаков, что дает хорошие результаты, только если корреляционная зависимость между признаками примерно одинакова и не является очень высокой, т. е. признаки следует группировать. Однако при сильном искривлении пространства признаков количество ошибочных решений остается слишком большим (см. рис. 4, *в*). На практике корреляционная зависимость между признаками различна.

Мера близости и мета-признаки Байеса — Минковского

Корреляция не только искривляет пространство признаков, но и несет в себе дополнительную информацию об образах, которая «переносится» в «скрытые» измерения. Чтобы извлечь данную информацию, предложена мера Байеса — Минковского [1]

$$y = \sqrt[g]{\sum_{j=1}^{n} \left| \left| \frac{(m_t - a_t)}{\sigma_t} \right|^g - \left| \frac{(m_j - a_j)}{\sigma_j} \right|^g \right|}, j \neq t. \qquad (3)$$

Эта метрика принимает тем меньшие значения, чем выше $C_{j,t}$.

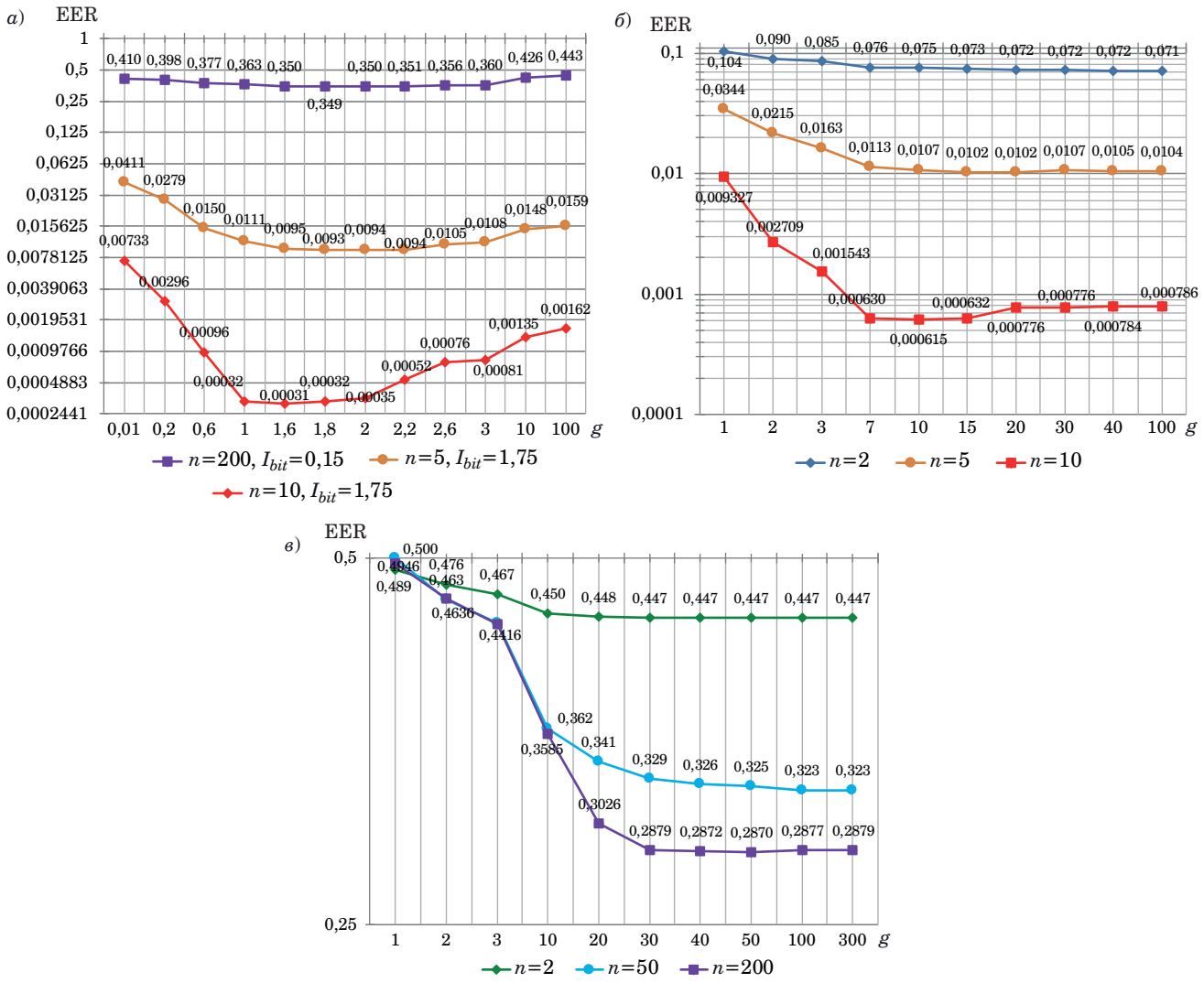
Собственная информация, которая содержится в признаках и рассчитывается по формуле (2), и та, что содержится в их корреляционных связях, различны. Чтобы показать это, в данной работе проведен еще один эксперимент по распознаванию образов мерой Байеса — Минковского (3) с условиями, аналогичными предыдущему эксперименту. Из представленных данных (рис. 5, *а–г*) видно, что оптимум g для меры (3) меняется в каждом рассмотренном случае. Если признаки независимы, то минимум по EER достигается при $g > 1$, если существенно коррелированы — при $0{,}7 \le g \le 1$.

Динамика изменения EER для меры Байеса — Минковского имеет обратную тенденцию по сравнению с показателями EER для меры Минковского. Если признаки коррелированы, мера Байеса — Минковского дает в разы более высокий результат, чем при независимых признаках. Причем вероятность ошибок распознавания в пространстве сильно коррелированных ($C \approx 0{,}9$) признаков для меры Байеса — Минковского ниже (см. рис. 5, *в*), чем уровень ошибок для меры Минковского в случае независимости признаков (см. рис. 4, *а*) при той же информативности и количестве признаков ($I_{bit} \approx 0{,}15$ и $n = 200$).

Таким образом, мера Байеса — Минковского является «антагонистом» по отношению к мере Минковского, так как обладает противоположными свойствами. Кроме того, мы видим, что информативность I_{bit} влияет на результат, как и корреляция C, и это влияние не взаимоисключающее (информативные признаки дают более хороший результат, чем малоинформативные, даже при отсутствии корреляции, но при ее наличии результат еще лучше). Соответственно, *информация о различии классов образов, которая содержится в признаках и их корреляционных связях, не дублируется*.

Под мета-признаком далее понимается выражение

$$a'_\iota = a'_{t,j} = f(a_t, a_j) = \left| a_t - a_j \right|,$$
$$j > t, \iota = \sum_{i=1}^{t-1} (n - i) + j - t. \qquad (4)$$



■ ***Рис. 4.*** Влияние g и n на EER (мера Минковского): *а* — признаки независимы ($C = 0$), различная информативность; *б* — признаки информативны ($I_{bit} \approx 1{,}75$), слабо зависимы ($C \approx 0{,}1$); *в* — признаки малоинформативны ($I_{bit} \approx 0{,}15$), сильно зависимы ($C \approx 0{,}9$)

■ ***Fig. 4.*** Effect of g and n on EER (Minkowski measure): *а* — the features are independent ($C = 0$), different information content; *б* — the features are informative ($I_{bit} \approx 1.75$), weakly dependent ($C \approx 0.1$); *в* — the features are little informative ($I_{bit} \approx 0.15$), highly dependent ($C \approx 0.9$)

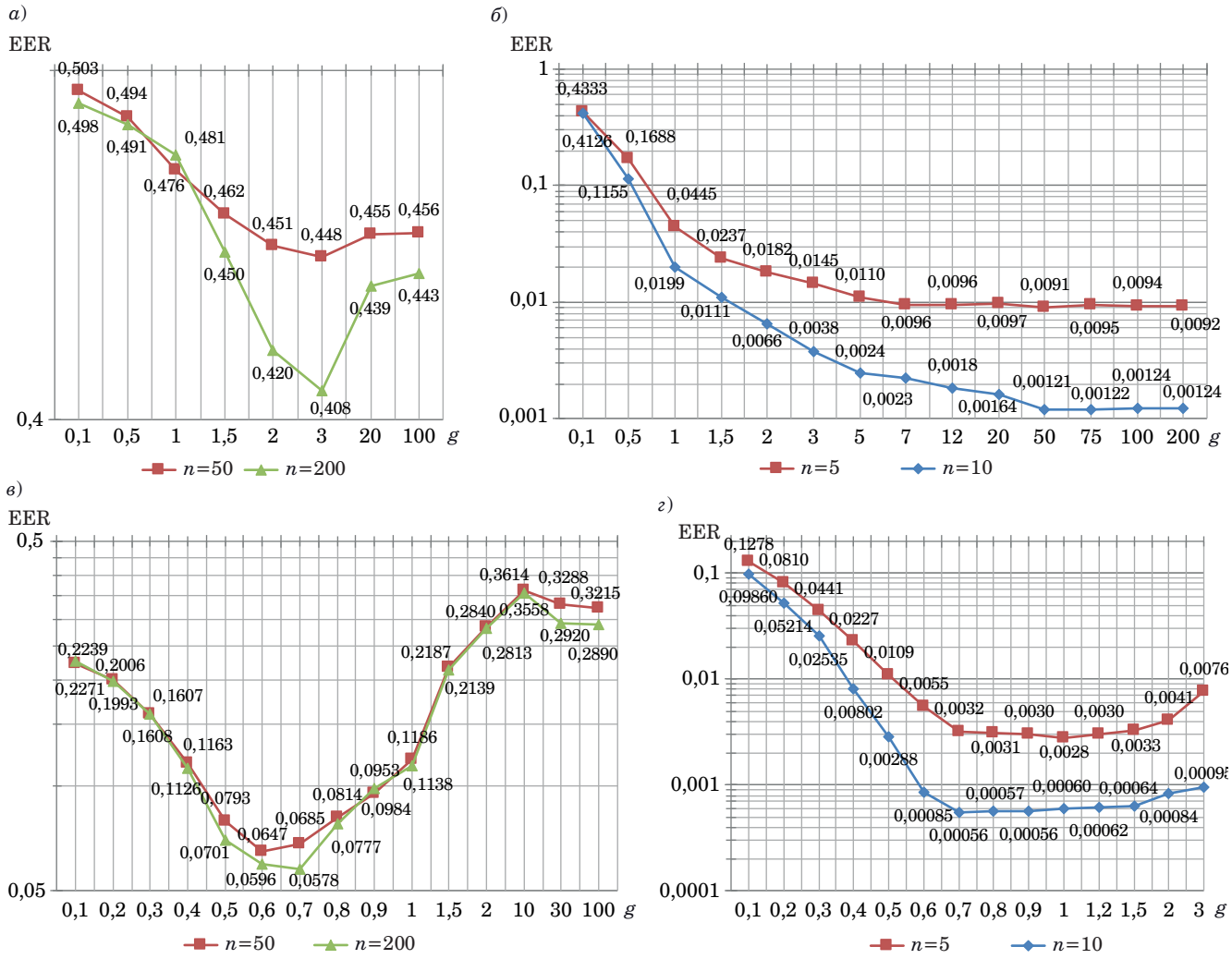
Чем меньше $|a'_{j,t}|$, тем выше внутриклассовая корреляция между признаками j и t, если $C_{j,t} = 1$, то $a'_{t,j} \approx 0$ при условии, что области значений признаков нормированы и центрированы. Размерность пространства мета-признаков Байеса — Минковского составляет

$$n' = 0{,}5(n(n-1)) = 0{,}5n^2 - 0{,}5n.$$

Мера Байеса — Минковского (3) — это линейный классификатор в пространстве мета-признаков, подобных (4), но нормирующих и центрирующих их значения относительно образов «Свой» с учетом априорных знаний параметров m_j и σ_j. Проблема метрики (3) в том, что параметры m_j и σ_j компрометируют информацию о классе образов «Свой». Без этих параметров мера близости на первый взгляд обладает меньшей информацией, однако не все так однозначно. Классификация образов возможна и без знаний m_j и σ_j.

Модель корреляционного нейрона и алгоритм обучения НПБК

Пусть корреляционный нейрон соединяется с мета-признаками (4), которые были порождены парами признаков с сильной взаимной корреляцией. Один мета-признак может быть связан только с одним корреляционным нейроном во избежание реализации атак, основанных на поиске общих связей нейронов [12, 15]. Введем два уровня коррелированности признаков: $C_{\_} = -0{,}5 > C_{j,t}$



■ ***Рис. 5.*** Влияние g и n на EER (мера Байеса — Минковского): *а* — признаки независимы (C=0) и малоинформативны ($I_{bit} \approx 0{,}15$); *б* — признаки независимы (C=0) и весьма информативны ($I_{bit} \approx 1{,}75$); *в* — признаки сильно коррелированы (C=0,9) и малоинформативны ($I_{bit} \approx 0{,}15$); *г* — признаки слабо коррелированы (C=0,1) и информативны ($I_{bit} \approx 1{,}75$)

■ ***Fig. 5.*** Effect of g and n on EER (Bayes — Minkowski measure): *а* — the features are independent (C=0) and uninformative ($I_{bit} \approx 0.15$); *б* — the features are independent (C=0) and very informative ($I_{bit} \approx 1.75$); *в* — the features are highly correlated (C=0.9) and uninformative ($I_{bit} \approx 0.15$); *г* — the features are weakly correlated (C=0.1) and informative ($I_{bit} \approx 1.75$)

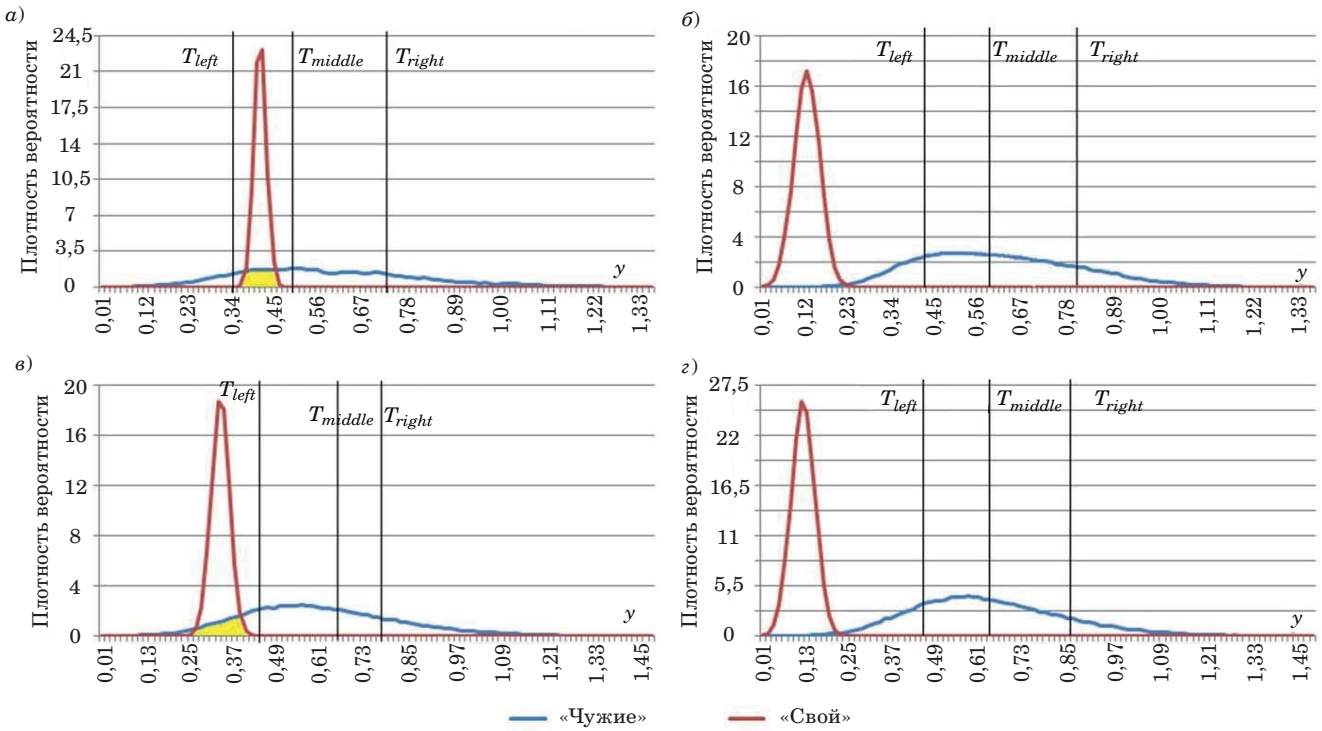
и $C_+ = 0{,}5 < C_{j,t}$. Корреляционный нейрон не должен быть связан с признаками, которые имеют уровень взаимной коррелированности $|C_{-+}| < 0{,}3$. Нейрон строится на базе метрики взвешенного среднеквадратичного отклонения (5) значений мета-признаков (4), которая позволяет отделить как положительно коррелированные, так и отрицательно коррелированные данные (рис. 6). Это происходит потому, что при наличии сильной положительной или отрицательной корреляции между исходными признаками выражение $|a'_\iota - m'|$ имеет тенденцию давать более низкие значения:

$$y = \sqrt{\frac{1}{\eta}\sum_{\iota=1}^{n'} w_\iota \left(a'_\iota - m'\right)^2}, \qquad (5)$$

$$m' = \frac{\sum_{\iota^*=1}^{\eta} a'_{\iota^*}}{\eta},$$

где η — количество входов нейрона; w_ι — вес синапса под номером ι ($w_\iota \geq 0$; если $w_\iota = 0$, то ι-й мета-признак не соединяется с нейроном); ι^* — номер входа для сквозной нумерации (без учета входов, для которых $w_\iota = 0$). Вес синапса рассчитывается по формуле

$$w_\iota = \frac{\left|m''_{(G),\iota} - m''_{(I),\iota}\right|}{\sigma''_{(G),\iota} \cdot \sigma''_{(I),\iota}}, \qquad (6)$$



■ ***Рис. 6.*** Плотности вероятности значений меры (5) для сгенерированных данных после отображения (4) при $g = 1$, $I \approx 1{,}75$ бит: *а* — для всех классов $1 > C_{j,t} > 0{,}95$, $n' = 10$; *б* — для всех классов $-1 < C_{j,t} < -0{,}95$, $n' = 10$; *в* — для классов «Свой» $1 > C_{j,t} > 0{,}95$, для класса «Чужие» $|C_{j,t}| < 0{,}3$, $n' = 10$; *г* — для классов «Свой» $-1 < C_{j,t} < -0{,}95$, для класса «Чужие» $|C_{j,t}| < 0{,}3$, $n' = 10$

■ ***Fig. 6.*** Probability density graphs of the values of measure (5) for the generated data after display (4) with $g = 1$, $I \approx 1{,}75$ bits: *a* — for all classes $1 > C_{j,t} > 0{,}95$, $n' = 10$; *б* — for all classes $-1 < C_{j,t} < -0{,}95$, $n' = 10$; *в* — for the « Genuine» classes $1 > C_{j,t} > 0{,}95$, for the «Alien» class $|C_{j,t}| < 0{,}3$, $n'=10$; *г* — for the « Genuine» classes $-1 < C_{j,t} < -0{,}95$, for the «Alien» class $|C_{j,t}| < 0{,}3$, $n' = 10$

$$m''_{(G),\iota} = \frac{\sum_{k=1}^{K_G}\left(a''_{\iota,k} - m'\right)^2}{K_G},\quad m''_{(I),\iota} = \frac{\sum_{k=1}^{K_I}\left(a'_{\iota,k} - m'\right)^2}{K_I},$$

$$\sigma''_{(G),\iota} = \sqrt{\frac{\sum_{k=1}^{K_G}\left(\left(a'_{\iota,k} - m'\right)^2 - m''_{(G),\iota}\right)^2}{K_G}},$$

$$\sigma''_{(I),\iota} = \sqrt{\frac{\sum_{k=1}^{K_I}\left(\left(a'_{\iota,k} - m'\right)^2 - m''_{(I),\iota}\right)^2}{K_I}}.$$

После обучения нейрона параметры $m''_{(G),\iota}$, $m''_{(I),\iota}$, $\sigma''_{(G),\iota}$, $\sigma''_{(I),\iota}$ должны быть удалены.

Нейроны должны иметь четырехуровневую пороговую функцию активации

$$\phi(y) = \begin{cases} \text{"11"}, & y < T_{left} \\ \text{"10"}, & T_{left} \le y < T_{middle} \\ \text{"01"}, & T_{middle} \le y < T_{right} \\ \text{"00"}, & y \ge T_{right} \end{cases}, \qquad (7)$$

где T_{left}, T_{middle} и T_{right} — левый, средний и правый пороговые значения активации нейрона (см. рис. 6). В соответствии с предлагаемой моделью нейрон имеет четыре варианта активации {0, 1, 2, 3} и только один из них соответствует гипотезе «Свой», остальные соответствуют гипотезе «Чужие». О том, какое именно состояние активации соответствует гипотезе «Свой» (далее ϕ_G), известно только на этапе синтеза и обучения НПБК, злоумышленник не обладает этой информацией, так как она не сохраняется после настройки нейрона.

При поступлении образа «Свой» на выходе нейрона почти всегда должно возникать определенное состояние, а в других ситуациях состояния {0, 1, 2, 3} должны быть случайны. Поэтому для вычисления порогов необходимо рассчитать границы интервала значений откликов нейрона y на обучающие примеры «Свой» $[y_{G\,\min}, y_{G\,\max}]$ и «Чужие» $[y_{I\,\min}, y_{I\,\max}]$ по формуле

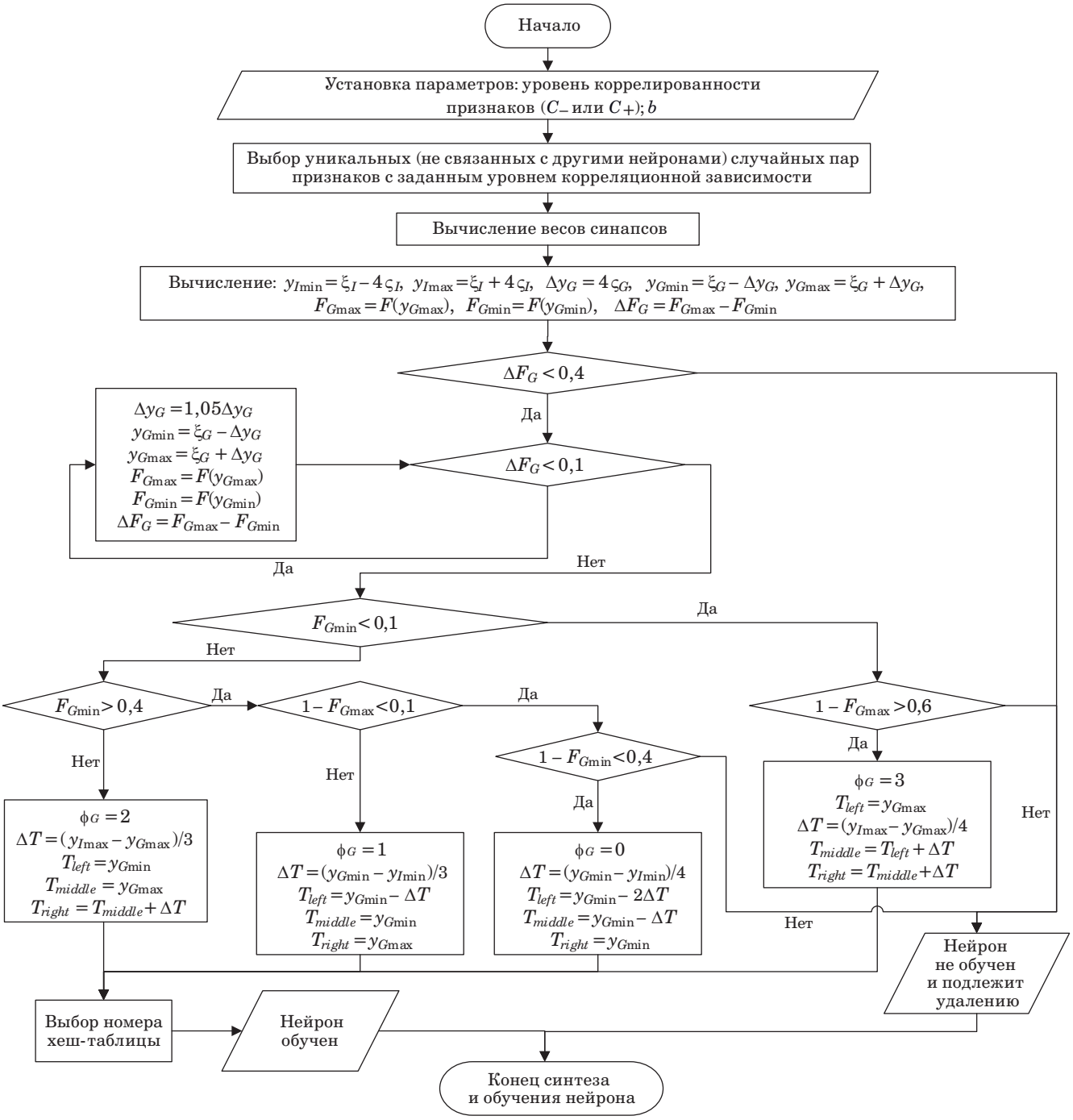
$$y_{\min} = \xi - 4\varsigma, y_{\max} = \xi + 4\varsigma \qquad (8)$$

и функции распределения нормального закона $F_G(y)$ и $F_I(y)$ [1]:

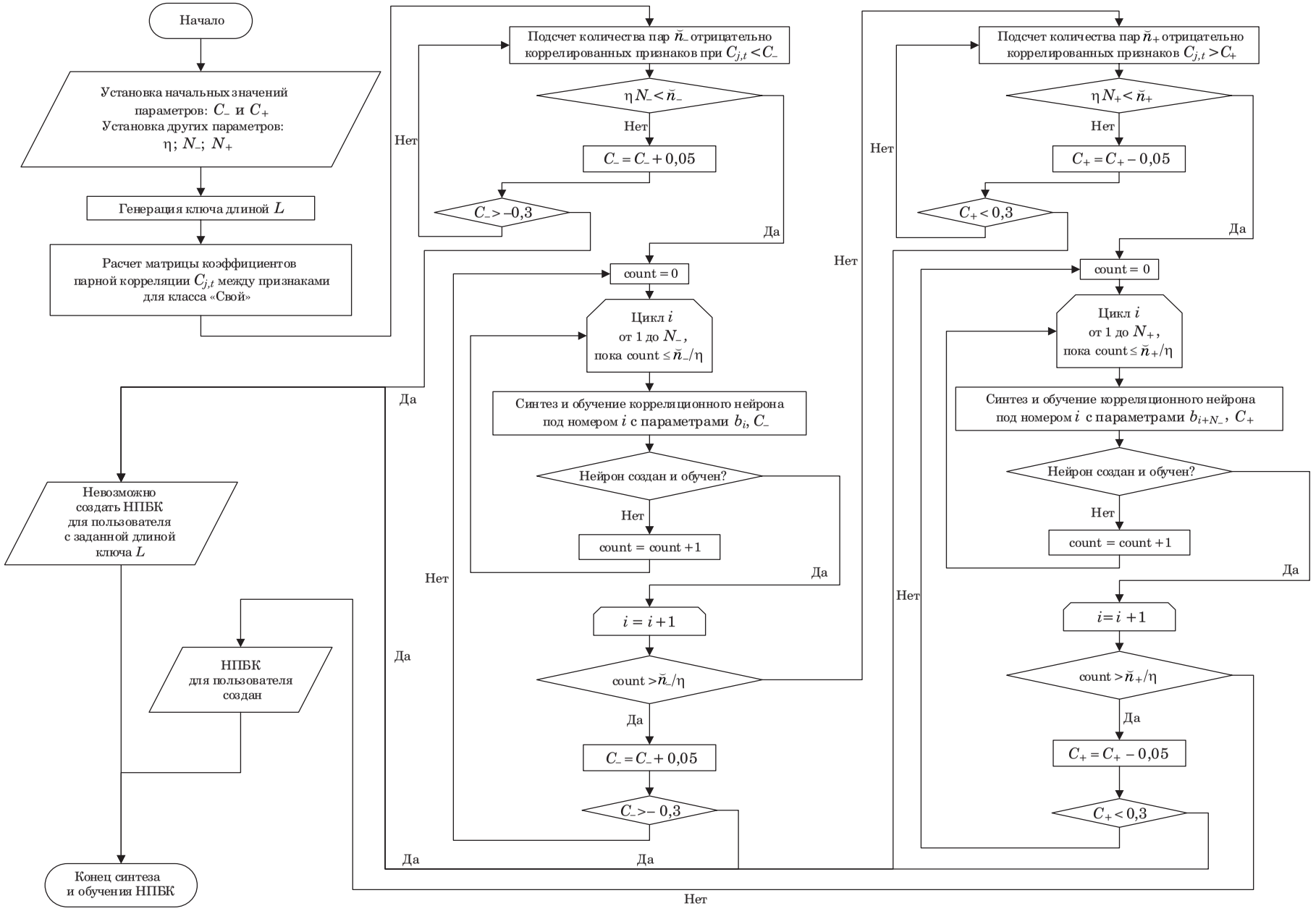
$$F(y) = \int_{-\infty}^{y} \frac{1}{\varsigma\sqrt{2\pi}} e^{-\frac{(\zeta-\xi)^2}{2\varsigma^2}} \mathrm{d}\zeta, \qquad (9)$$

где ξ и ς — математическое ожидание и среднеквадратичное отклонение величины y при поступлении на входы нейрона обучающих примеров «Свой» или «Чужие».

Исходя из гипотезы о нормальном распределении y, подтвержденной методом хи-квадрат [1], каждый нейрон будет давать ложный отказ пользователям «Свой» с вероятностью, в среднем не превышающей 0,002. Однако в силу наличия корреляции между откликами различных нейронов показатели FRR и FAR невозможно просчитать заранее без проведения численного эксперимента.



■ ***Рис. 7.*** Алгоритм синтеза и обучения корреляционного нейрона
■ ***Fig. 7.*** Algorithm for synthesis and training of a correlation neuron



■ ***Рис. 8.*** Алгоритм синтеза и обучения НПБК

■ ***Fig. 8.*** Algorithm for synthesis and training of biometrics-code converter

Настройка порогов нейрона выполняется по модифицированному алгоритму (рис. 7, базовый алгоритм представлен в работе [1]).

Выходы кодировщика должны быть преобразованы в мета-признаки (4), которые должны быть связаны с НПБК. При регистрации нового пользователя для него создается отдельный НПБК, который обучается на примерах «Свой» и «Чужие» в доверенной среде в соответствии с алгоритмом, представленным на рис. 8. После обучения НПБК может размещаться в открытом виде.

Таблицы порогов T весовых коэффициентов w_i обученного НПБК представляют собой защищенный эталон пользователя.

Эксперименты по распознаванию голосовых образов

При проведении эксперимента использованы предложенные модели предварительно обученных нами автокодировщиков, модель НПБК на базе корреляционных нейронов, предложенный алгоритм ее обучения (см. рис. 8) и сформированный в рамках настоящей работы набор данных.

При оценке на собственной базе для обучения каждого НПБК использовано по 20 примеров «Свой» голосового образа определенного пользователя, находящегося в нормальном состоянии, а также по одному примеру всех остальных пользователей из группы «Зарегистрированные субъекты» в качестве тренировочной выборки «Чужие» (всего 64 примера «Чужих»). При оценке на базе RedDots для обучения использовано по 10 примеров «Свой» и 239 примеров «Чужих».

Для тестирования НПБК и определения вероятности ошибок «ложного отказа» «Своему» (FRR) использованы образы «Свой», не участвовавшие в обучении. Эта серия опытов выполнялась дважды: сначала с использованием образов, полученных на первом этапе сбора данных, когда состояние пользователей было нормальным (без дрейфа), потом с использованием образов, полученных позже в измененных состояниях субъектов (в условиях дрейфа).

Для тестирования стойкости НПБК к попыткам входа со стороны злоумышленника и определения вероятности ошибок «ложного допуска» (FAR) использованы примеры из группы «Неизвестные Чужие» для оценки на собственной базе (и «Imposters» для оценки на RedDots). Результаты тестирования можно видеть в табл. 1 и 2.

Балансировка показателей FRR и FAR возможна за счет использования кодов, исправляющих ошибки, например кодов Безяева [24]. С их помощью можно исправить определенное количество ошибок в формируемом на выходе НПБК ключе и таким образом установить порог принятия биометрического образа.

Нейросетевой преобразователь биометрия-код на базе корреляционных нейронов дает гораздо меньший процент ошибок и в разы большую длину ключа, чем классический НПБК на базе алгоритма обучения ГОСТ Р 52633.5. Влияние состояния субъекта на результаты аутентификации при использовании предложенной модели НПБК менее существенны, чем для классической модели. Полученные результаты можно объяснить тем, что если дрейфующие характеристики голоса коррелированы, то они изменяются схожим образом. Другими словами, корреляция между существенной частью дрейфующих признаков сохраняется. По этой причине корреляционные нейроны являются относительно устойчивыми к дрейфу голосовых образов.

Из представленных результатов видно, что предложенная модель дает уровни ошибок и точ-

■ ***Таблица 1.*** Результаты эксперимента с собственной базой дикторов (EER, %)
■ ***Table 1.*** Experimental results with its own base of speakers (EER, %)

η	Предложенная модель НПБК при количестве нейронов N				НПБК, обучаемый по ГОСТ Р 52633.5, при количестве нейронов N			
	512		1024		128		256	
	1	2	1	2	1	2	1	2
2	–	–	–	–	7,73	8,91	5,27	7,9
4	4,31	5,38	3,7	4,69	7,46	10,73	–	–
6	3,64	4,73	3,47	4,41	–	–	–	–
7	3,42	4,46	3,33	4,31	–	–	–	–
8	3,66	4,72	3,26	4,33	–	–	–	–
9	3,75	4,76	3,48	4,42	–	–	–	–

Примечание: Столбцы 1 — дрейфа нет; столбцы 2 — дрейф есть.

■ ***Таблица 2.*** Результаты эксперимента с набором данных RedDots
■ ***Table 2.*** Experimental results with RedDots dataset

Методы и модели	EER, %	Точность,%
Комплексирование нескольких моделей и методов (модель гауссовой смеси, i-, x-vector) [25]	2,77	–
Вейвлет-преобразование, нейронная сеть и преобразование Гильберта [26]	–	95,1
MFCC + глубокая нейронная сеть [27]	1,61	–
Глубокие скрытые марковские модели (DHMM) [28]	–	97,6
Иерархическая многослойная акустическая модель (HiLAM) [29]	1,02	–
Предложенная модель НПБК (η =6, N = 4096)	2,64	97,36

ности, сопоставимые с мировым уровнем. Однако стоит учитывать, что в настоящем исследовании дополнительно ставится задача не только защиты от дрейфа, но и защиты биометрических шаблонов от компрометации, а также обеспечения автоматического и робастного обучения при регистрации нового пользователя. Все указанные свойства одновременно не обеспечиваются ни одной из указанных моделей, с которыми осуществлялось сравнение по базе RedDots.

Заключение

Полученные результаты показали, что есть преимущества от использования корреляционных нейронов в задачах голосовой биометрии:

– данные о классе «Свой» не компрометируются, так как их не требуется хранить в виде параметров распределения значений признаков;

– НПБК на базе корреляционных нейронов дает меньший процент ошибок (почти на 60 %) и большую длину ключа (в четыре раза) по сравнению с НПБК на базе ГОСТ Р 52633.5. Количество ошибок составило: EER = 3,26 % (для предложенной модели) при длине ключа 1024 бит и EER = 5,27 % (для классической модели) при длине ключа 256 бит;

– если дрейфующие признаки сильно коррелированы, то обычно они сдвигаются синхронно по диагонали (чаще всего в рамках линии расширения пространства признаков, см. рис 5, *б*), при этом значение мета-признака меняется несущественно. Эксперимент показал, что это справедливо, так как вероятности ошибок повышаются в среднем на 25–30 % (для классической модели повышение количества ошибок при изменении состояния пользователя колеблется от 15 до 50 %);

– предложенная модель не уступает существующим аналогам по точности, при этом существующие модели не обеспечивают защиту биометрических шаблонов и автоматическое обучение при регистрации нового пользователя, о чем свидетельствуют эксперименты на открытой базе RedDots.

Дальнейшие исследования будут направлены на создание гибридных моделей нейронных сетей, способных выполняться в защищенном режиме, и НПБК на их основе. Если объединить классические нейроны с другими типами нейронов в гибридный слой нейронов, синтезировав гибридную нейронную сеть, можно снизить показатели FRR и FAR и повысить энтропию ответов НПБК. Еще более интересным является то, что создание многослойных гибридных нейронных сетей, где в каждом слое будут использованы различные типы нейронов, может также позволить снизить вероятность ошибочных решений и открыть новые перспективы.

Финансовая поддержка

Работа выполнена ОмГТУ в рамках государственного задания Минобрнауки России на 2023–2025 годы № FSGF-2023-0004.

Литература

1. **Sulavko A. E.** Biometric-based key generation and user authentication using acoustic characteristics of the outer ear and a network of correlation neurons. *Sensors*, 2022, vol. 22, pp. 9551. doi:10.3390/s22239551
2. **Иванов А. И., Князьков В. С.** Перспектива многократного увеличения ресурсов доверенных вычислений за счет привлечения гибрида нейросетевой обработки биометрии и гомоморфного шифрования. *Состояние и перспективы развития современной науки по направлению «Техническое зрение, распознавание образов»: материалы III Всерос. науч.-техн. конф.*, Анапа, 18 марта 2021 г. Анапа, 2021, с. 173–176. EDN: WFBSXO
3. **Catak F. O., Yayilgan S. Y., Abomhara M.** A privacy-preserving fully homomorphic encryption and parallel computation based biometric data matching. *Preprints*

2020, No. 2020070658. doi:10.20944/preprints202007.0658.v1

4. **Barrero G. M., Maiorana E., Galbally J., Campisi P., Fierrez J.** Multi-biometric template protection based on Homomorphic Encryption. *Pattern Recognition*, 2017, vol. 67, pp. 149–163.
5. **Torres W. A. A., Bhattacharjee N., Srinivasan B.** Effectiveness of fully homomorphic encryption to preserve the privacy of biometric data. *Proc. of the 16th Intern. Conf. on Information Integration and Web-based Applications & Services (iiWAS '14)*, N. Y., USA, 2014, pp. 152–158. doi:https://doi.org/10.1145/2684200.2684296
6. **Sudhakar T., Gavrilova M.** Cancelable biometrics using deep learning as a cloud service. *IEEE Access*, 2020, vol. 8, pp. 112932–112943. doi:10.1109/ACCESS.2020.3003869
7. **El-Shafai W., Mohamed F. A. H. E., Elkamchouchi H. M., Abd-Elnaby M., Elshafee A.** Efficient and secure cancelable biometric authentication framework based on genetic encryption algorithm. *IEEE Access*, 2021, vol. 9, pp. 77675–77692.
8. **Ponce-Hernandez W., Blanco-Gonzalo R., Liu-Jimenez J., Sanchez-Reillo R.** Fuzzy vault scheme based on fixed-length templates applied to dynamic signature verification. *IEEE Access*, 2020, vol. 8, pp. 11152–11164.
9. **Rathgeb C., Merkle J., Scholz J., Tams B., Nesterowicz V.** Deep face fuzzy vault: Implementation and performance. *Computers & Security*, 2022, vol. 113, Article 102539.
10. **Иванов А. И.** *Нейросетевая защита конфиденциальных биометрических образов гражданина и его личных криптографических ключей*: монография. Пенза, ПНИЭИ, 2014. 57 с.
11. **Ахметов Б. С., Иванов А. И., Фунтиков В. А., Безяев А. В., Малыгина Е. А.** *Технология использования больших нейронных сетей для преобразования нечетких биометрических данных в код ключа доступа*: монография. Алматы, Издательство LEM, 2014. 144 с.
12. **Marshalko G. B.** On the security of a neural network-based biometric authentication scheme. *Математические вопросы криптографии*, 2014, т. 5, № 2, с. 87–98. EDN: TKJPFV
13. **Иванов А. И., Крохин И. А.** Таблица вероятности появления разных стартовых условий для атак Маршалко на нейроны с общими входными связями. *Состояние и перспективы развития современной науки по направлению «Техническое зрение, распознавание образов»: материалы III Всерос. науч.-техн. конф.*, Анапа, 18 марта 2021 г. Анапа, 2021, с. 171–172.
14. **Сулавко А. Е.** Высоконадежная двухфакторная биометрическая аутентификация по рукописным и голосовым паролям на основе гибких нейронных сетей. *Компьютерная оптика*, 2020, т. 44, № 1, с. 82–91. doi:10.18287/2412-6179-CO-567, EDN: OVLPUD
15. **Bogdanov D. S., Mironkin V. O.** Data recovery for a neural network-based biometric authentication scheme. *Математические вопросы криптографии*, 2019, т. 10, № 2, с. 61–74.
16. **Сулавко А. Е., Еременко А. В., Борисов Р. В., Иниватов Д. П.** Влияние психофизиологического состояния диктора на параметры его голоса и результаты биометрической аутентификации по речевому паролю. *Компьютерные инструменты в образовании*, 2017, № 4, с. 29–47.
17. **Sheluhin O. I., Erokhin S. D., Osin A. V., Barkov V. V.** Experimental studies of network traffic of mobile devices with Android OS. *IEEE Conf. "Systems of Signals Generating and Processing in the Field of on Board Communications"*, Moscow, Russia, 20–21 March 2019. IEEE, 2019, pp. 1–4. doi:10.1109/SOSG.2019.8706824
18. **Sheluhin O. I., Barkov V. V., Sekretarev S. A.** The online classification of the mobile applications traffic using data mining techniques. *T-Comm*, 2019, vol. 13, no. 10, pp. 60–67. doi:10.24411/2072-8735-2018-10317.1
19. **Николенко С. И., Кадурин А. А., Архангельская Е. О.** *Глубокое обучение. Погружение в мир нейронных сетей*. СПб., Питер, 2018. 480 с.
20. **Lee K. A., Larcher A., Wang G., Kenny P., Brümmer N., van Leeuwen D., Aronowitz H., Kockmann M., Vaquero C., Ma B., Li H., Stafylakis T., Alam M. J., Swart A., Perez J.** The reddots data collection for speaker recognition. *Proc. Interspeech 2015*, 2015, pp. 2996–3000. doi:10.21437/Interspeech.2015-95
21. **Snyder D., Garcia-Romero D., Sell G., Povey D., Khudanpur S.** X-vectors: Robust DNN embeddings for speaker recognition. *IEEE Intern. Conf. on Acoustics, Speech and Signal Processing (ICASSP)*, Calgary, AB, Canada, 15–20 April 2018. IEEE, 2018, pp. 5329–5333. doi:10.1109/ICASSP.2018.8461375
22. **Nagrani A., Chung J. S., Xie W., Zisserman A.** Voxceleb: Large-scale speaker verification in the wild. *Computer Speech & Language*, 2020, vol. 60, Article 101027.
23. **Дагаева М. В., Катасева Д. В., Катасев А. С.** Аугментация данных и построение нейросетевых моделей распознавания рукописных символов в системах биометрической аутентификации. *Информация и безопасность*, 2018, т. 21, № 3, с. 366–371.
24. **Безяев А. В.** Биометрико-нейросетевая аутентификация: обнаружение и исправление ошибок в длинных кодах без накладных расходов на избыточность: препринт. Пенза, Изд-во ПГУ, 2020. 40 с.
25. **Sarkar A. K., Tan Z. H.** *On bottleneck features for text-dependent speaker verification using X-vectors*. arXiv preprint arXiv:2005.07383. 2020.
26. **Sarma K., Pyrtuh F., Chakraborty D.** Speaker verification system using wavelet transform and neural network for short utterances. *Asian Journal*

for Convergence in Technology (AJCT), 2020, vol. 6, no. 1, pp. 30–35.
27. **Sarkar A. K., Tan Z. H.** Self-segmentation of pass-phrase utterances for deep feature learning in text-dependent speaker verification. *Computer Speech & Language*, 2021, vol. 70, Article 101229.
28. **Arora S. V., Vig R.** An efficient text-independent speaker verification for short utterance data from Mobile devices. *Multimedia Tools and Applications*, 2020, vol. 79, pp. 3049–3074.
29. **Laskar M. A., Laskar R. H.** HiLAM-state discriminative multi-task deep neural network in dynamic time warping framework for text-dependent speaker verification. *Speech Communication*, 2020, vol. 121, pp. 29–43.

UDC 004.93'1
doi:10.31799/1684-8853-2024-2-21-38
EDN: YIVAYM

Authentication based on voice passwords with the biometric template protection using correlation neurons

A. E. Sulavko[a], PhD, Tech., Associate Professor, orcid.org/0000-0002-9029-8028, sulavich@mail.ru
D. P. Inivatov[a], Assistant Professor, https://orcid.org/0000-0001-9911-1218
V. I. Vasilyev[b], Dr. Sc., Tech., Professor, orcid.org/0000-0002-6105-5481
P. S. Lozhnikov[a], Dr. Sc., Tech., Professor, orcid.org/0000-0001-7878-1976
[a]Omsk State Technical University, 11, Mira Pr., 644050, Omsk, Russian Federation
[b]Ufa University of Science and Technology, 32, Z. Validi St., 450076, Ufa, Russian Federation

Introduction: The issue of protecting biometric data from compromise is closely related to performance issues. Existing methods of biometric voice authentication either do not protect voice data from compromise or give a high percentage of erroneous decisions; in addition, they do not provide resistance to voice image drift. **Purpose:** To develop a method of biometric voice authentication that is resistant to the drift of biometric data while ensuring the confidentiality of voice parameters. **Results:** We propose an authentication method using neural network "biometrics-to-code" converters based on a modified model of correlation neurons and their training algorithms. It has been established that correlations between features contain information about images that does not duplicate the information contained in the features. The biometrics-to-code converter based on correlation neurons produces a much lower percentage of errors and several times longer key length than the classical model based on the GOST R 52633.5 learning algorithm. The number of errors was: 3.26%. When the subject's state changes (intoxication or sleepiness), the number of errors for the developed method does not increase as significantly as for the classical model of the biometrics-code neural network converter. **Practical relevance:** The results can be used to increase the security of computer resources from unauthorized access and biometric data from compromise. **Discussion:** Combining neurons of various types into a single layer will make it possible to create more stable and reliable biometric-to-code neural network converters.

Keywords — secure execution of neural network algorithms, processing of correlated biometric features, voice biometrics, neural network biometrics-to-code converters, time series analysis, autoencoders.

For citation: Sulavko A. E., Inivatov D. P., Vasilyev V. I., Lozhnikov P. S. Authentication based on voice passwords with the biometric template protection using correlation neurons. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2024, no. 2, pp. 21–38 (In Russian). doi:10.31799/1684-8853-2024-2-21-38, EDN: YIVAYM

Financial support
The research was supported by Ministry of Science and Higher Education of the Russian Federation (theme No. FSGF-2023-0004).

References

1. Sulavko A. E. Biometric-based key generation and user authentication using acoustic characteristics of the outer ear and a network of correlation neurons. *Sensors*, 2022, vol. 22, pp. 9551. doi:10.3390/s22239551
2. Ivanov A. I., Knyazkov V. S. The prospect of a multiple increase in trusted computing resources by involving a hybrid of neural network processing of biometrics and homomorphic encryption. *Materialy III Vseros. nauch.-tekhn. konf. «Sostoyanie i perspektivy razvitiya sovremennoj nauki po napravleniyu "Tekhnicheskoe zrenie, raspoznavanie obrazov"»* [Proc. III All-Russian Scient.-Tech. Conf. «The State and prospects of development of modern science in the direction of "Technical vision, pattern recognition"»], Anapa, 2021, pp. 173–176 (In Russian). EDN: WFBSXO
3. Catak F. O., Yayilgan S. Y., Abomhara M. A privacy-preserving fully homomorphic encryption and parallel computation based biometric data matching. *Preprints* 2020, No. 2020070658. doi:10.20944/preprints202007.0658.v1
4. Barrero G. M., Maiorana E., Galbally J., Campisi P., Fierrez J. Multi-biometric template protection based on Homomorphic Encryption. *Pattern Recognition*, 2017, vol. 67, pp. 149–163.
5. Torres W. A. A., Bhattacharjee N., Srinivasan B. Effectiveness of fully homomorphic encryption to preserve the privacy of biometric data. *Proc. of the 16th Intern. Conf. on Information Integration and Web-based Applications & Services (iiWAS '14)*, N. Y., USA, 2014, pp. 152–158. doi:https://doi.org/10.1145/2684200.2684296
6. Sudhakar T., Gavrilova M. Cancelable biometrics using deep learning as a cloud service. *IEEE Access*, 2020, vol. 8, pp. 112932–112943. doi:10.1109/ACCESS.2020.3003869
7. El-Shafai W., Mohamed F. A. H. E., Elkamchouchi H. M., Abd-Elnaby M., Elshafee A. Efficient and secure cancelable biometric authentication framework based on genetic encryption algorithm. *IEEE Access*, 2021, vol. 9, pp. 77675–77692.
8. Ponce-Hernandez W., Blanco-Gonzalo R., Liu-Jimenez J., Sanchez-Reillo R. Fuzzy vault scheme based on fixed-length templates applied to dynamic signature verification. *IEEE Access*, 2020, vol. 8, pp. 11152–11164.
9. Rathgeb C., Merkle J., Scholz J., Tams B., Nesterowicz V. Deep face fuzzy vault: Implementation and performance. *Computers & Security*, 2022, vol. 113, pp. 102539.

10. Ivanov A. I. *Neirosetevaia zashchita konfidentsial'nykh biometricheskikh obrazov grazhdanina i ego lichnykh kriptograficheskikh kliuchei* [Neural Protection of Sensitive Biometric Images of the Citizen and his Personal Cryptographic Keys]. Penza, PNIEI Publ., 2014. 57 p. (In Russian).
11. Ahmetov B. S., Ivanov A. I., Funtikov V. A., Bezjaev A. V., Malygina E. A. *Tekhnologiia ispol'zovaniia bol'shikh neironnykh setei dlia preobrazovaniia nechetkikh biometricheskikh dannykh v kod kliucha dostupa* [Technology of Using Large Neural Networks for Fuzzy Transformation of Biometric Data in the Access Code Key]. Almaty, LEM Publ., 2014. 144 p. (In Russian).
12. Marshalko G. B. On the security of a neural network-based biometric authentication scheme. *Mathematical Aspects of Cryptography*, 2014, vol. 5, no. 2, pp. 87–98. EDN: TKJPFV
13. Ivanov A. I., Krokhin I. A. Table of the probability of occurrence of different starting conditions for Marshalko attacks on neurons with common input connections. *Materialy III Vseros. nauch.-tekhn. konf. «Sostoyanie i perspektivy razvitiya sovremennoj nauki po napravleniyu "Tekhnicheskoe zrenie, raspoznavanie obrazov"»* [Proc. III All-Russian Scient.-Tech. Conf. «The State and prospects of development of modern science in the direction of "Technical vision, pattern recognition"»], Anapa, 2021, pp. 171–172 (In Russian).
14. Sulavko A. E. Highly reliable two-factor biometric authentication by handwritten and voice passwords based on flexible neural networks. *Computer optics*, 2020, vol. 44, no. 1, pp. 82–91 (In Russian). doi:10.18287/2412-6179-CO-567, EDN: OVLPUD
15. Bogdanov D. S., Mironkin V. O. Data recovery for a neural network-based biometric authentication scheme. *Mathematical Aspects of Cryptography*, 2019, vol. 10, no. 2, pp. 61–74.
16. Sulavko A. E., Eremenko A. V., Borisov R. V., Inivatov D. P. Influence of a speaker's psycho-physiological state to his voice parameters and results of biometric authentication by speech enabled password. *Computer Tools in Education*, 2017, no. 4, pp. 29–47 (In Russian).
17. Sheluhin O. I., Erokhin S. D., Osin A. V., Barkov V. V. Experimental studies of network traffic of mobile devices with Android OS. *IEEE Conf. "Systems of Signals Generating and Processing in the Field of on Board Communications"*, Moscow, Russia, 20–21 March 2019. IEEE, 2019, pp. 1–4. doi:10.1109/SOSG.2019.8706824
18. Sheluhin O. I., Barkov V. V., Sekretarev S. A. The online classification of the mobile applications traffic using data mining techniques. *T-Comm*, 2019, vol. 13, no. 10, pp. 60–67. doi:10.24411/2072-8735-2018-10317.1
19. Nikolenko S. I., Kadurin A. A., Arkhangelskaya E. O. *Glubokoe obuchenie. Pogruzhenie v mir nejronnyh setej* [Deep learning. Dive into the world of neural networks]. Saint-Petersburg, Piter Publ., 2018. 480 p. (In Russian).
20. Lee K. A., Larcher A., Wang G., Kenny P., Brümmer N., van Leeuwen D., Aronowitz H., Kockmann M., Vaquero C., Ma B., Li H., Stafylakis T., Alam M. J., Swart A., Perez J. The reddots data collection for speaker recognition. *Proc. Interspeech 2015*, 2015, pp. 2996–3000. doi:10.21437/Interspeech.2015-95
21. Snyder D., Garcia-Romero D., Sell G., Povey D., Khudanpur S. X-vectors: Robust DNN embeddings for speaker recognition. *IEEE Intern. Conf. on Acoustics, Speech and Signal Processing (ICASSP)*, Calgary, AB, Canada, 15–20 April 2018. IEEE, 2018, pp. 5329–5333. doi:10.1109/ICASSP.2018.8461375
22. Nagrani A., Chung J. S., Xie W., Zisserman A. Voxceleb: Large-scale speaker verification in the wild. *Computer Speech & Language*, 2020, vol. 60, Article 101027.
23. Dagaeva M. V., Kataseva D. V., Katasev A. S. Data augmentation and construction of neural network models for handwritten character recognition in biometric authentication systems. *Informaciya i bezopasnost'*, 2018, vol. 21, no. 3, pp. 366–371 (In Russian).
24. Bezyaev A. V. *Biometriko-neyrosetevaya autentifikatsiya: obnaruzhenie i ispravlenie oshibok v dlinnykh kodakh bez nakladnykh raskhodov na izbytochnost'* [Bio-metrical neural network authentication: detecting and correcting errors in long codes without the overhead of redundancy]. Penza, PGU Publ., 2020. 40 p. (In Russian).
25. Sarkar A. K., Tan Z. H. *On bottleneck features for text-dependent speaker verification using X-vectors*. arXiv preprint arXiv:2005.07383. 2020.
26. Sarma K., Pyrtuh F., Chakraborty D. Speaker verification system using wavelet transform and neural network for short utterances. *Asian Journal for Convergence in Technology (AJCT)*, 2020, vol. 6, no. 1, pp. 30–35.
27. Sarkar A. K., Tan Z. H. Self-segmentation of pass-phrase utterances for deep feature learning in text-dependent speaker verification. *Computer Speech & Language*, 2021, vol. 70, Article 101229.
28. Arora S. V., Vig R. An efficient text-independent speaker verification for short utterance data from Mobile devices. *Multimedia Tools and Applications*, 2020, vol. 79, pp. 3049–3074.
29. Laskar M. A., Laskar R. H. HiLAM-state discriminative multi-task deep neural network in dynamic time warping framework for text-dependent speaker verification. *Speech Communication*, 2020, vol. 121, pp. 29–43.

UDC 004.056
doi:10.31799/1684-8853-2024-2-39-50
EDN: YXVAJI

Articles

Security assessment based on attack graphs using NVD and MITRE ATT & CK database for heterogeneous infrastructures

R. O. Kryukov[a], *PhD, Tech., Lecturer, orcid.org/0009-0008-3422-7234*
E. V. Fedorchenko[b], *PhD, Tech., Senior Researcher, orcid.org/0000-0001-6707-9153*
I. V. Kotenko[b], *Dr. Sc., Tech., Professor, orcid.org/0000-0001-6859-7120, ivkote@comsec.spb.ru*
E. S. Novikova[b], *PhD, Tech., Associate Professor, orcid.org/0000-0003-2923-4954*
V. M. Zima[a], *PhD, Tech., Professor, orcid.org/0009-0006-9412-4160*
[a]*A. F. Mozhaiskii Military Space Academy, 13, Zhdanovskaia Emb., 197198, Saint-Petersburg, Russian Federation*
[b]*St. Petersburg Federal Research Center of the RAS, 39, 14th Line, 199178, Saint-Petersburg, Russian Federation*

Introduction: *Security assessment of modern information systems is a challenging task. These systems incorporate heterogeneous objects, things, subjects and connections between them. They are continuously changing and generate a lot of events. As a result, the system security state is constantly changing.* ***Purpose:*** *To develop an approach for security assessment of the heterogeneous information systems.* ***Results:*** *We develop and present an approach to security assessment. It incorporates data gathering from various sources, log preprocessing, security incidents detection, mapping the security incidents to the nodes of the attack graph, security assessment and forecasting, and results representation. The novelty of the proposed approach is in the technique for mapping the detected incidents to the stages of the targeted cyber attacks. This technique uses the Emerging Threats correlation rules to output the security incidents based on the detected events. It also uses the Targeted Attack Analyzer (Indicators of Attack) rules that describe security incidents (signatures) using Sigma language to map the detected security incidents to the attack patterns from the MITRE ATT & CK database. Thus, the proposed technique allows one to map the detected events to the attack graph nodes and assess and forecast the targeted cyber attacks. The attack graph is generated using MITRE ATT & CK attack patterns and vulnerabilities from the National Vulnerability Database. The approach is implemented in the Python language. The test environment is deployed to test the mapping of the detected security incidents to the known attack patterns.* ***Practical relevance:*** *The investigation results can be used in the construction of security assessment systems that are aimed at strengthening cyber security of heterogeneous information systems.*

Keywords *— security assessment, cyber security incidents, event correlation, signature, cyber attack, attack graph, MITRE ATT & CK, National Vulnerability Database, targeted attack analyzer, indicators of attack, emerging threats.*

For citation: Kryukov R. O., Fedorchenko E. V., Kotenko I. V., Novikova E. S., Zima V. M. Security assessment based on attack graphs using NVD and MITRE ATT & CK database for heterogeneous infrastructures. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2024, no. 2, pp. 39–50. doi:10.31799/1684-8853-2024-2-39-50, EDN: YXVAJI

Introduction

Currently, digitalization covers more and more areas of human life. Along with advantages, it leads to new threats. Thus, supporting information technology infrastructure is vulnerable to cyber threats. Their successful implementation can lead to such consequences as power outage that is uncomfortable for people and crucial for the industry, for example, water treatment, medical infrastructures, etc.

Modern information technology infrastructures are characterized by a high level of complexity and heterogeneity. Security information and event management systems (SIEM) were introduced to monitor the system's processes and to detect malicious ones. These systems allow early attack detection and forecasting and provide security incident forensics utilities. SIEM systems collect events from different sources and implement their correlation analysis to support these tasks. The event correlation in information security allows revealing the dependencies between the events relating to the same cyber security incident [1]. It incorporates the following stages: normalization, preprocessing, anonymization, aggregation, filtering, correlation itself, and prioritization [1]. The event correlation results are the cyber security incidents. They are used by the researchers to attribute the attacker [2–4], forecast the attack development, and select measures for countering cyber attacks.

In this paper, the authors focus on the targeted cyber attacks as multi-step and hard-to-detect attacks. A targeted attack is a type of cyber attack that is aimed at compromising a specific system or object. Such attacks can have different development vectors (techniques). They incorporate the following standard stages: reconnaissance, resource development, initial access, execution, persistence, privilege escalation, defense, evasion, credential access, and discovery. The stages may vary depending on

the object under attack. The consequences of the targeted cyber attack can be crucial. Detection of cyber attack at an early stage can help avoid considerable damage. Both attack detection and prevention require event correlation. It allows detection of the cyber security incident and mapping it to the appropriate attack stage and technique for further prevention.

The researchers proposed various event correlation techniques for the SIEM systems based on the manual [5], supervised [6], and unsupervised methods [7, 8]. Existing information security monitoring tools implement these techniques. At the same time, while most security monitoring tools allow detecting cyber security incidents using correlation techniques, they do not allow mapping the detected security incidents to the targeted cyber attack stages. To fill the gap, the paper [9] introduced the technique based on the set of Emerging Threats (https://rules.emergingthreats.net/open/suricata-5.0/rules/) correlation rules and on the set of Targeted Attack Analyzer (Indicators of Attack) (TAA (IOA)) rules (https://support.kaspersky.com/KATA/3.7.1/en-US/194907.htm). The set of Emerging Threats correlation rules is applied for events correlation to output cyber security incidents. The set of TAA (IOA) rules is used to map the detected security incidents to the stages of the targeted cyber attacks. The TAA (IOA) rules describe behavior in the system (signature) that could indicate a targeted attack (security incident) and can be validated in real time [10, 11]. The authors [9] use the open dataset of the TAA (IOA) rules specified in Sigma language (https://github.com/SigmaHQ/sigma/tree/master/rules) and integrated with the MITRE ATT & CK database (https://attack.mitre.org/). The IOA allows mapping the security incidents (signatures) to the attack stages from the MITRE ATT & CK database, namely, reconnaissance, resource development, initial access, execution, persistence, privilege escalation, defense, evasion, credential access, and discovery. The technique proposed in [9] allows detecting the security incidents based on the security events and mapping them to the IOA mapped to the MITRE ATT & CK tactics and techniques. The research was presented at the 5th International Workshop on Attacks and Defenses for the Internet-of-Things (ADIoT 2022).

In this paper, the authors describe the common approach to security assessment based on attack graphs using the National Vulnerability Database (NVD, https://nvd.nist.gov/) and MITRE ATT & CK database that incorporates the technique presented in [9] as one of the stages. The authors also introduce a novel attack graph model that integrates attack stages represented using MITRE ATT & CK objects and attack actions represented using the vulnerabilities from the NVD, and security assessment technique based on the proposed attack graph and mapping of the security incidents to this graph. The proposed approach allows forecasting of the next attack steps, and in prospect, it will allow timely responses against cyber attacks.

The main *contributions* of the paper are as follows:

– the approach to security assessment of the information systems using NVD and MITRE ATT & CK database. It is based on attack graphs. The developed approach uses the technique for detecting and mapping the cyber security incidents presented in [9] as one of the stages;

– a novel attack model in the form of the attack graph, constructed considering cyber attack stages and vulnerabilities of the system under analysis;

– the security assessment technique. It is based on the developed attack graph and the mapping of the security incidents to the generated graph.

The *novelty* of the proposed solution is as follows:

– the comprehensive approach to the security assessment using NVD and MITRE ATT & CK and considering mapping of the security incidents to the cyber attack stages. It uses the technique for detecting and mapping the cyber security incidents presented in [9] as one of the stages;

– the attack graph that differs by the joint consideration of the attack stages and attack actions;

– the security assessment technique based on the proposed attack graph and mapping of the security incidents to the graph.

Related research

Currently, a wide variety of event correlation techniques has been proposed [8]. They could be classified into three main groups according to the knowledge extraction method: manual, supervised, and unsupervised. Rules and signature-based approaches form the first group, while the second and third groups include corresponding machine-learning techniques and algorithms. Despite their variety, their primary goal is to generate security incidents based on observed system, network, and application events.

Such techniques are used in SIEM systems to detect anomalous activity. Thus, Splunk Enterprise Security (https://www.splunk.com/en_us/products/enterprise-security.html) uses correlation based on the trained neural network to detect anomalies in the event stream using the trained neural network. QRadar SIEM (https://www.ibm.com/qradar/security-qradar-siem), HP ArcSight Security Intelligence (http://www.microfocus.com/en-us/cyberres/secops/arcsight-esm), and MaxPatrol SIEM (https://www.ptsecurity.com/ww-en/products/mpsiem/) use rule-based correlation methods.

Few security solutions implement further mapping of the security events and accidents to the indicators of attacks. This functionality is often implemented as an additional component, and is based on expert rules. For example, PT Network Attack Discovery component (https://mitre.ptsecurity.com/en-US/techniques?utm_source=pt-main-en&utm_medium=slider&utm_campaign=mitre) from Positive Technologies implements automated mapping of the detected incidents to a set of the attack techniques and tactics. SIEM QRadar from IBM includes QRadar Use Case Manager. It provides functionality for the generation of rules to map the detected incidents to specific tactics and techniques.

There is a public knowledge-based repository of adversary tactics and techniques — the MITRE ATT & CK repository. It incorporates more than 620 attack techniques for enterprise information platforms. The provided tactics, techniques, and procedures are classified by the attack stages. Another recent MITRE research effort, D3FEND, attempts to link known countermeasures to corresponding attack techniques. One of the most common ways to use MITRE ATT & CK matrix is modeling attack paths to determine missed attack steps and appropriate countermeasures [12–14]. For example, in [14], a methodology for a system security assessment based on the attacker's behaviour modeling is presented. The attacker's behaviour is represented as a sequence of techniques specified in the MITRE ATT & CK matrix.

In [12], authors propose a new structure that links the attack graph and attack kill chain steps. As the attack graph is constructed for a given system configuration, the proposed structure maps the given system to the possible attack steps and recommended countermeasures. The mapping of the MITRE ATT & CK techniques to the attack graph elements is implemented using a ruleset defined manually.

Xiong et al. developed a threat modeling language that allows modeling attacks in the system being analyzed [13]. It enables the specification of the information system entities. Then the textual descriptions of the MITRE ATT & CK techniques are manually mapped to language structures that link system entities, attack techniques, and countermeasures, making it possible to reveal available countermeasures for each attack step and define missed ones.

In [15], authors focused on the problem of the probabilistic generation of the attack steps represented by the MITRE ATT & CK tactics. They use a hidden Markov model to represent transitions between tactics and techniques and try to calculate transition probabilities based on the analysis of the observable events. A set of observables is extracted from over 25 documents and other materials relating to the incidents in the industrial control systems. This analysis allowed the authors to determine the frequency of transitions between tactics and techniques and to transform them in initial probabilities, transition probabilities, and observable emission probabilities. The authors demonstrated that it is possible to generate different attack scenarios by changing the probabilities.

In [16–18] MITRE ATT & CK matrix serves as a basis for stating and validating hypotheses about attacks and their paths based on observations revealed by an analyst and historical data about attacks and threat actions. For example, in [16] the authors construct a graph of attack tactics and evaluate different algorithms for predicting missing graph edges and vertices to discover missed attack steps. The source data for constructing such an attack graph are data about attacks that are available through the MITRE ATT & CK STIX repository. Al-Shaer et al. investigated the problem of the similarity of different attack scenarios to reveal inter-dependencies between techniques and tactics. They demonstrated that certain fine-grained associations between techniques and tactics could be used to forecast an attacker's behavior [18].

A. Nisioti et al. propose DISCLOSE, a framework targeted to support the forensics investigation and evaluate the severity of the security breaches [17]. Similarly to [16], the authors use the MITRE ATT & CK STIX repository to construct a knowledge graph that reflects the probabilistic dependencies between attack techniques and could be used to reveal missed attack steps and forecast attack steps. Moreover, the authors suggest evaluating the cost and benefit of each attack action. The benefit of the attack actions is determined based on their properties, such as required privileges and user interaction, using the Common Vulnerability Scoring System Base Score Calculator. The cost of the attack actions is calculated based on expert assessments. Thus, the analyst may understand the impact of the possible attack actions using numerical scores and select appropriate countermeasures.

In [19], Kim et al. adopt the MITRE ATT & CK matrix to implement mobile advanced persistent threat attribution. They propose to form a vectorized presentation of tactics based on the results of their similarity analysis. The authors demonstrated that such a solution allows a reduction of the false positive rate in task of malware author's attribution.

The approach proposed in this paper is close to the approach suggested in [17]. But unlike the approach [17], the introduced approach performs security incident mapping to attack patterns in real-time mode and considers the step of the event correlation and construction of the security incidents and alerts.

Approach for security assessment based on attack graphs using NVD and MITRE ATT & CK database

Cyber attack incorporates several stages that are called kill chain. As soon as we consider enterprise networks, the stages are as follows: reconnaissance, resource development, initial access, execution, persistence, privilege escalation, defense evasion, credential access, discovery, lateral movement, collection, command and control, exfiltration, and impact. Some of them can be missed. Besides, to implement each stage several techniques can be used.

Detection of cyber attacks at the early stages of the kill chain allows for a reduced impact on the target system. In this paper, we propose an approach to security assessment based on attack graphs using NVD and MITRE ATT & CK database. The goal is to enhance the results of the security assessment via enhancement of the targeted attack detection. It can be specified as follows: $Res_{PA} \geq Res_{EA}$, where *Res* is defined as the number of the detected attack stages for the proposed approach (Res_{PA}) and existing approaches (Res_{EA}).

The proposed approach incorporates data gathering from various sources; log preprocessing; security incidents detection using correlation analysis; mapping the security incidents to the nodes of the attack graph constructed considering the kill chain using NVD and MITRE ATT & CK database; security assessment and forecasting based on the constructed graph; and results representation (Fig. 1). It takes as input the security incidents and outputs the risk scores for the resources of the analyzed system. The stages of the approach are detailed in the subsections below.

Data gathering and log preprocessing

First, in the data gathering stage, the raw data from the network log *net_log* and the internal log *syslog* (or other) are gathered. These data enter the preprocessing stage.

In the preprocessing stage, the raw data D_r are normalized, preprocessed, filtered, and aggregated (Fig. 2) using the following algorithm.

Step 1. The raw data D_r, i. e. the set of network and internal events, enter the normalization process *Norm*. D_r are converted to the normalized format in terms of length and syntax:

$$D_r \overset{read}{\rightarrow} Norm(len, syn),$$

where *len* — the fixed length; *syn* — the normalized event syntax.

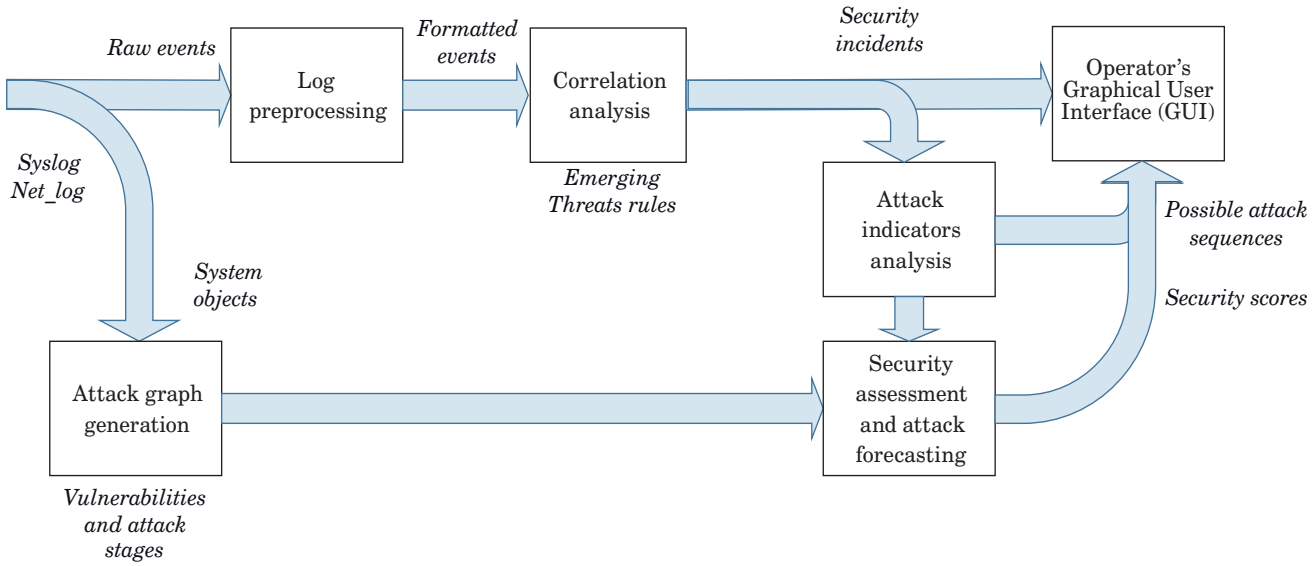
Step 2. The normalized events enter the preprocessing *Proc*. The events are supplemented by the fields essential for the correlation: *time_start*, *time_end*, *list*:

$$D_r \overset{read}{\rightarrow} Proc(time\_start, time\_end, list),$$

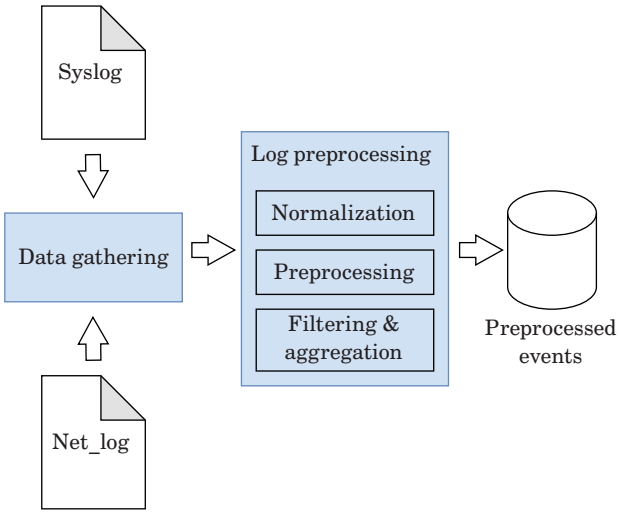
where *time_start* — event start time; *time_end* — event end time; *list* — event source.

Step 3. The preprocessed events enter the filtering and aggregation process *Filter*. It is required to remove the repeated events and aggregate similar events:

$$D_r \overset{read}{\rightarrow} Filter(del\_attr, meta),$$



■ ***Fig. 1.*** The generalized scheme of the proposed approach



■ ***Fig. 2.*** The scheme of the data gathering and log preprocessing process

where *del_atr* – a function for the removal of repeated events; *meta* – a function for aggregation of similar events.

Limitations:

$$\{C_1, C_2, ..., C_n\} \cup \{L_1, L_2, ..., L_k\} \in D,$$

where C – network events; L – internal events (events from operation system log); D – preprocessed events.

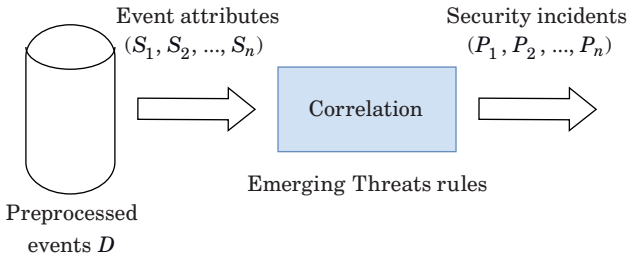
Security incident detection using correlation analysis

Correlation allows security incident detection. At this stage, the Emerging Threats correlation rules are used for events correlation (Fig. 3).

The authors specify the correlation rule as the following mathematical object:

$$< Rule\_type > [< TriG > (S_1, S_2, ..., S_n) \overset{impact}{\rightarrow} (P_1, P_2, ..., P_k) \overset{display}{\rightarrow} < Alert >, < Severity >],$$

where <*Rule_type*> – a type of the correlation rule that depends on the event source *list*. We outline the following types of correlation rules: *App-layer*, *Decoder*, *Dhcp*, *Dnp3*, *DNS*, *Files*, *http2*, *http*, *Ipsec*, *Kerberos*, *Modbus*, *Mqtt*, *Nfs*, *Smb*, *Tls*; <*TriG*> – the security incidents signatures, several signatures can exist for the same type of correlation rule; (S_1, S_2, ..., S_n) – event attributes indicating the security incidents; (P_1, P_2, ..., P_k) – detected security incidents; <*Alert*> – alert for the cyber security incident; <*Severity*> – severity of the alert (low, medium, or high).



■ ***Fig. 3.*** The scheme of security incident detection using log correlation analysis

This is the production model that uses IF-THEN rules to represent an operation. The preprocessed events D enter the correlation analysis (see Fig. 3). The event source *list* is used to select the correlation rule. The event attributes S trigger alert *Alert* if they correspond to one or several signatures *TriG* of the security incidents P. The severity of the alert depends on the number of security incidents. The algorithm for correlation can be specified as follows.

Step 1. Events D enter the correlation rule depending on their source *list*:

$$D \overset{read}{\rightarrow} Rule\_type.$$

Step 2. The events syntax represented by the event attributes S, is mapped to the features specified within the cyber security incident signature *TriG*:

$$D \overset{read}{\rightarrow} < Rule\_type >< TriG > (S_1, S_2, ..., S_n).$$

Step 3. If the events D contain at least one attribute corresponding to the feature specified in the cyber security incident signature, then the incident is detected:

$$D \overset{read}{\rightarrow} < Rule\_type >< TriG > (S_1, S_2, ..., S_n) \overset{impact}{\rightarrow} (P_1, P_2, ..., P_k).$$

Step 4. The alert *Alert* is generated and sent to the operator's GUI together with its severity:

$$D \overset{read}{\rightarrow} < Rule\_type > [< TriG > (S_1, S_2, ..., S_n) \overset{impact}{\rightarrow} (P_1, P_2, ..., P_k) \overset{display}{\rightarrow} < Alert >, < Severity >].$$

The obtained security incidents are passed to the attack indicators analysis stage.

Technique for mapping the security incidents to the nodes of the attack graph

At this stage, the security incidents obtained using events correlation are mapped to the cyber attack stages represented as an attack graph. The graph is generated considering the MITRE ATT & CK tactics and techniques, i. e. to the stages of the targeted cyber attacks.

The cyber attacks model represented as an attack graph, and a set of TAA (IOA) rules are used for this goal.

The attack graph is specified considering the analyzed system and cyber attack stages.

The analyzed system is specified based on its objects *Obj* and relations between them *Rel* as follows:

$$S = \{Obj, Rel\}.$$

Each object $obj \in Obj$ is specified as follows:

$$obj = \{ip\_addr, type, software, hardware\}.$$

Object type *type* is specified considering the submatrices of the Enterprise matrix of the MITRE ATT & CK (https://attack.mitre.org/matrices/enterprise/) as follows:

$$type \in \{PRE, Windows, macOS, Linux, Cloud, Network, Containers\}.$$

It is used to specify applicable attack stages and to determine the object's criticality.

Software *software* and hardware *hardware* are used to detect the object's vulnerabilities and generate attack subgraphs.

Rel specifies relations between objects.

The generalized attack graph *GAG* is specified as the set of attack subgraphs *ASG* and connections *Con* between them:

$$GAG = \{ASG, Con\}.$$

Each subgraph *ASG* is specified depending on the type *type* of the system object *Obj* under attack as the set of the attack stage nodes *stage*:

$$ASG = \bigcup_{i=1}^{n} stage_i,$$

where n — is the number of the attack stages that depend on *type*. For example, for the *type* = *Windows* (https://attack.mitre.org/matrices/enterprise/windows/), *ASG* = {*Initial Access*, *Execution*, *Persistence*, *Privilege Escalation*, *Defense*, *Evasion*, *Credential Access*, *Discovery*, *Lateral Movement*, *Collection*, *Command and Control*, *Exfiltration*, *Impact*}, while for the *type* = *PRE* (https://attack.mitre.org/matrices/enterprise/pre/), *ASG* = {*Reconnaissance*, *Resource*, *Development*}.

Each stage *stage* is specified as a stage attack subgraph considering *type*:

$$stage = \{N, Con, Pr\},$$

where N — the set of stage attack graph nodes; *Con* — the set of connections between them; *Pr* — probability of successful stage implementation.

Each node $n \in N$ represents an attack action. It is specified as follows:

$$n = \{V, Pr\},$$

where V — the set of vulnerabilities that can be used to implement the attack action; *Pr* — probability of successful attack action implementation.

The set of vulnerabilities is specified considering the *type* of the system *obj*, its *hardware*, and *software*. The vulnerabilities are related to attack *stages* if an appropriate connection exists in the MITRE ATT & CK database. Analysis of the MITRE ATT & CK databases demonstrated the low connectivity between this database and vulnerability databases (such as NVD). Thus, this research proposes using the technique for classification of the vulnerabilities by the MITRE ATT & CK stages using machine learning methods.

The TAA (IOA) rules describe security incidents (signatures) using Sigma language. The IOA allows mapping the security incidents to the attack stages from the MITRE ATT & CK database, for example, reconnaissance, resource development, initial access, execution, persistence, privilege escalation, defense, evasion, credential access, and discovery. The mapping is specified as follows:

$$< Sign > [< attack > (P_1, P_2, ..., P_n) \overset{display}{\rightarrow} < 0, 1 >, < R, MITRE_{obj} >],$$

where ⟨*Sign*⟩ — TAA (IOA) signatures of the security incidents; ⟨*attack*⟩ — attack techniques according to the MITRE ATT & CK. For example, it can take the following values: *Ddos_attack*, *Malv_attack*, *Scan_attack*, *Web_attack*, *Sql_attack*, *XSS_attack*, *Shell_attack*, *Dos_attack*, *Brut_attack*, *Pass_attack*, *Inject_attack*; (P_1, P_2, ..., P_n) — cyber security incidents corresponding to the attack technique; <0, 1> — the result of mapping of the security incidents (P_1, P_2, ..., P_n) to the MITRE ATT & CK techniques ⟨*attack*⟩ based on the signature ⟨*Sign*⟩: 0 — the set of the detected incidents (P_1, P_2, ..., P_n) do not correspond to the ⟨*Sign*⟩, 1 — the set of the detected incidents (P_1, P_2, ..., P_n) correspond to the ⟨*Sign*⟩; $MITRE_{obj}$ — attack description, its stage, possible

next steps, and attack responses according to the MITRE ATT & CK.

This process can be briefly described as follows. The signatures of the security incidents detected on the correlation stage are compared with the TAA (IOA) signatures of the same incidents. The targeted attack represented using MITRE ATT & CK techniques is detected if they match. Otherwise, the detected incident can't be mapped to the multi-step targeted attack represented with the path of the attack graph GAG. The attack responses depend on the attack stage and used tactics and techniques. Mapping the security incidents to the attack stages allows for assessing security, attack forecasting, and, in the future, selection of efficient attack responses.

The corresponding algorithm is as follows.

Step 1. Comparison of the signatures of the security incidents P_1, P_2, ..., P_n obtained from the D attributes using the Emerging Threats correlation rules with TAA (IOA) signatures. The TAA (IOA) signatures *Sign* of the incidents P_1, P_2, ..., P_n correspond to the tactics, techniques and procedures *attack* from the MITRE ATT & CK database. The comparison is specified as follows:

$$D(P_1, P_2, ..., P_k) \overset{compare}{\rightarrow}$$
$$< Sign >< attack > (P_1, P_2, ..., P_n).$$

Step 2. Displaying the $MITRE_{obj}$ if the signatures match:

$$D(P_1, P_2, ..., P_k) \overset{compare}{\rightarrow}$$
$$< Sign > [< attack > (P_1, P_2, \ ..., \ P_n) \overset{display}{\rightarrow}$$
$$< 1 > , \ < MITRE_{obj} >],$$

where 1 indicates that the set of the detected incidents P_1, P_2, ..., P_n correspond to the *Sign*. Go to Step 3. Otherwise, go to Step 4.

Step 3. Starting security assessment process.

Step 4. The security incident can not be mapped to the MITRE ATT & CK stages.

Security assessment

This research proposes a hierarchical security assessment process using a security risk score. A security risk score is calculated considering the probability of the security incident and the impact of the incident. It incorporates the following levels of hierarchy (from the lowest to the highest): 1) stage *stage* attack subgraph level — incorporates security risk scores for the *stage* attack subgraph nodes that are represented with attack actions n implemented using vulnerabilities; 2) *ASG* level — incorporates security risk scores for the *ASG* nodes that are represented with kill chain stages *stage*; 3) *GAG* level — incorporates security risk scores for the nodes of the *GAG* that are represented with *ASG*.

On the attack subgraph level, the approach described in [1] is used to calculate probabilities of successful attack actions *Pr*. The probability of attack is calculated using the equation for the unconditional probability:

$$\Pr(n_k) = \prod_{i=1}^{k} Pc(n_i \mid Pa[n_i]),$$

where n_k — the successful implementation of the k-th attack action represented using the attack graph node; *Pc* — local conditional probability distributions, i. e. the probability of compromise of a node considering the states of its parents; $Pa[n_k]$ — all parents of node n_k.

The graph traversal is used to calculate *Pr*.

Calculation of the unconditional probability requires the local conditional probability. To calculate local conditional probability distributions *Pc*, the approach proposed in [20] is used (the first equation for OR relations, the second equation — for AND relations):

$$Pc(n_k) = \begin{cases} 0 \text{ if } \forall n_i \in Pa[n_k] \mid n_i = \\ = 0 \text{ and } \left(1 - \prod_{i=1}^{k-1} (1 - Pc(n_i))\right) \text{ otherwise} \\ 0 \text{ if } \exists n_i \in Pa[n_k] \mid n_i = \\ = 0 \text{ and } \left(\prod_{i=1}^{k-1} (Pc(n_i))\right) \text{ otherwise} \end{cases},$$

where $n_i = 0$ means that attack action is not successful.

OR relations of the graph nodes (i. e. attack actions) represent the case when the successful implementation of the attack action requires the successful implementation of at least one of its parent nodes. AND relations of the graph nodes represent the case when the successful implementation of the attack action requires the successful implementation of all its parent nodes.

For the root node of the graph *Pc* is calculated using local probability $p(n)$ for this node:

$$Pc(n) = \begin{cases} p(n) & \text{for successful attack action} \\ 0 & \text{otherwise} \end{cases}.$$

The reverse depth-first traversal is used to calculate conditional probability distributions for all nodes.

The approach based on Common Vulnerability Scoring System metrics is used to calculate local

probabilities for the attack graph nodes and impact scores [1].

On the *ASG* level, the same approach is used but nodes are represented with kill chain stages *stage*. The local probabilities for the *stage* are calculated as probabilities *Pr* for the leaf nodes of the stage attack subgraph if it exists. If there is no stage attack subgraph for the *stage* (no corresponding vulnerabilities) then the local probability is calculated considering the complexity of the stage implementation according to the MITRE ATT & CK. Impact on this level is calculated as the maximum impact from the stage attack subgraph.

On the *GAG* level, the nodes are represented as *ASG*. Thus local probabilities are calculated as probabilities *Pr* for the leaf nodes of the *ASG*. Impacts are calculated considering the criticalities of the objects *Obj*.

In the case of security incidents, the probabilities for the nodes on all levels are recalculated considering Bayes' theorem.

Experiments

The authors implemented the proposed approach in Python programming language using the Flask framework (https://flask.palletsprojects.com/en/2.1.x/). Figure 4 provides the general architecture of the developed prototype.

The authors deployed the testing environment for the experiments. As the test case the small fragment of computer network was selected that can be the part of any supporting information technology infrastructure of power generation system. It is represented in Fig. 5. The developed prototype and the tested SIEM tools were installed on the Administrator's workstation.

The attacks were conducted against the user's workstation using internal tools of the Kali Linux operation system (https://www.kali.org/). The conducted attacks are provided in Table 1.

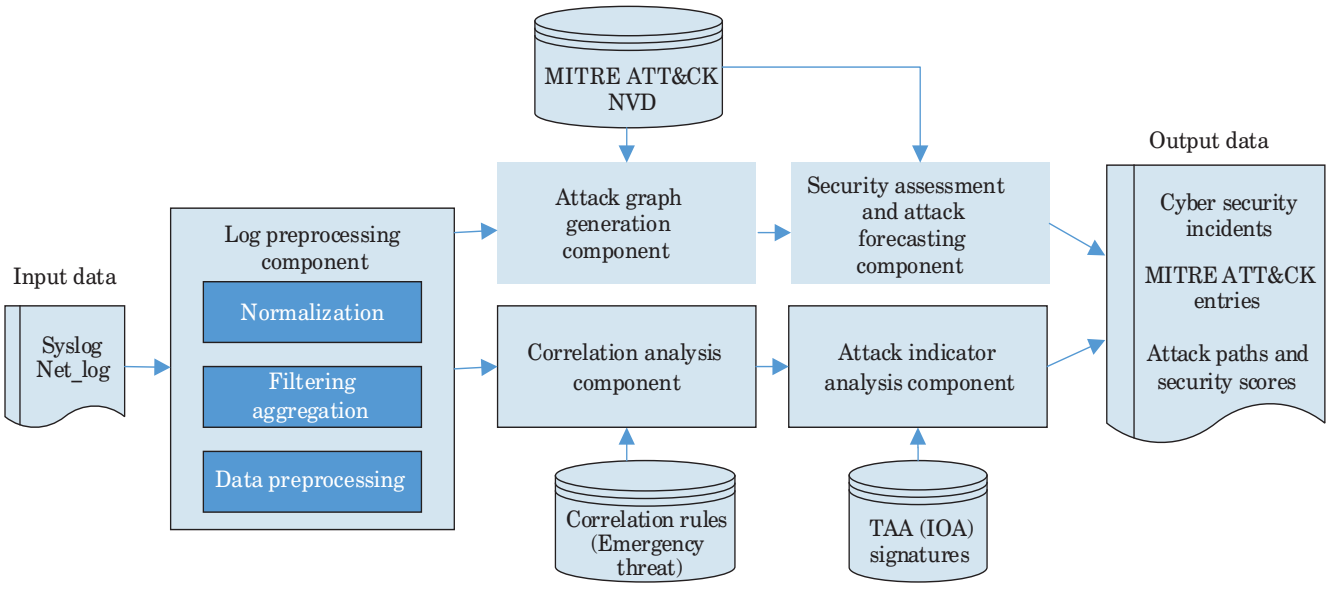
The Scan_attack is the first stage of the following attacks sequence (*TestSequence*): Reconnaissance (Scan_attack), Resource Development (Develop Capabilities), Initial Access (Exploit Public-Facing Application), Execution (Command and Scripting Interpreter), Persistence (Account Manipulation), Privilege Escalation (Scheduled Task), Defense Evasion (BITS Jobs), and Credential Access (Account Manipulation).

Table 2 contains the results of the experiments. It represents the following characteristics:

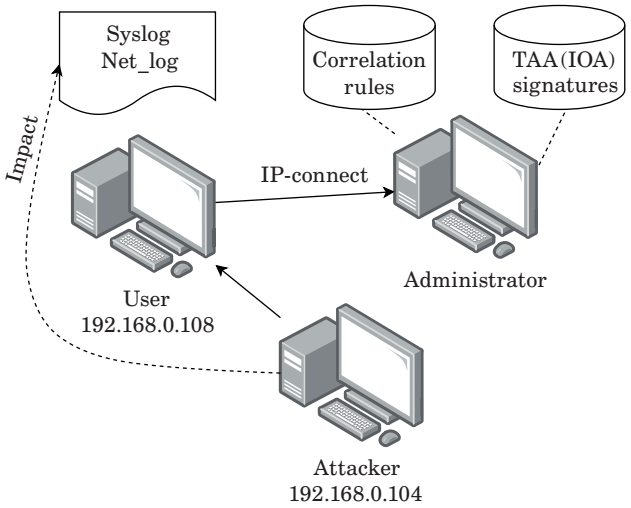
– the target IP-address;
– the conducted attacks;
– the types of events corresponding to the attacks (*C* – network events, *L* – operation system's log events);
– the TAA signatures corresponding to the attacks;
– the administrator IP-address;
– if the attack was detected and mapped.

Table 3 details the detected techniques for each attack according to the MITRE ATT & CK.

After detection and mapping of the attack to the attack sequence on the attack graph, the security risks are recalculated. Thus, the security risks for the TestSequence are provided in Fig. 6, where red color indicates high risk, yellow color – medium risk, and green color – low risk.



■ ***Fig. 4.*** General architecture of the developed prototype



■ ***Fig. 5.*** Deployed test environment

■ ***Table 1.*** The cyber attacks conducted within the test environment

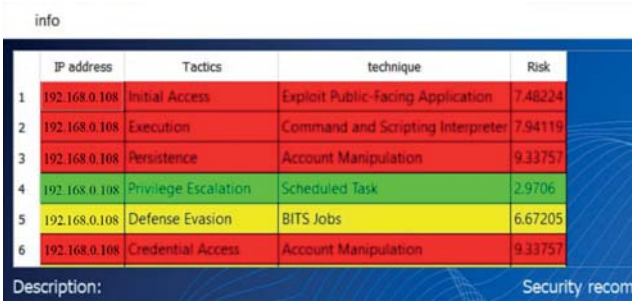
Attack	Source IP-address	Target IP-address	Success
Dos_impact	192.168.0.104 (Attacker)	192.168.0.108 (User)	+
Shell_impact	192.168.0.104 (Attacker)	192.168.0.108 (User)	+
Scan_impact	192.168.0.104 (Attacker)	192.168.0.108 (User)	+
Inject_impact	192.168.0.104 (Attacker)	192.168.0.108 (User)	+
Brut_impact	192.168.0.104 (Attacker)	192.168.0.108 (User)	+

■ ***Table 2.*** Successfully detected and mapped attacks

Attack	Event type	TAA signature	User IP-address	Administrator IP-address
Dos_ impact	*C*	Dos_ attack	192.168.0.108 (User)	127.0.0.1
Shell_ impact	*L*	Shell_attack	192.168.0.108 (User)	127.0.0.1
Scan_ impact	*C*	Scan_attack	192.168.0.108 (User)	127.0.0.1
Inject_ impact	*L*	Inject_ attack	192.168.0.108 (User)	127.0.0.1
Brut_ impact	*C* & *L*	Brut_attack	192.168.0.108 (User)	127.0.0.1

■ ***Table 3.*** The detected techniques of the conducted cyber attacks

Attack	Techniques according to the MITRE ATT & CK
Dos_impact	T1499.001, T1499.002, T1499.003, T1499.004
Shell_impact	T1505.001, T1505.002, T1505.003
Scan_impact	T1595.001, T1595.002



■ ***Fig. 6.*** The security risks for the TestSequence

Discussion and conclusion

The authors analyzed the modern SIEM systems and found out that they do not provide the functionality of the accurate mapping of the detected incidents to the attack stage for further security assessment and attack prevention. To fill this gap, the authors proposed a new approach to the security assessment incorporating a comprehensive technique for correlating the raw events into the security incidents and mapping the incidents to the attacks and attack stages. The information on the detected and mapped security incidents is further used in the scope of the security assessment technique. In the research, the authors used open source tools. The Emerging Threats correlation rules were used for event correlation. Mapping of the security incidents to the attack stages was implemented using the TAA (IOA) integrated with the MITRE ATT & CK database. NVD and MITRE ATT & CK databases were used for attack model generation. The authors developed their models and algorithms based on production rules, graph theory, probability theory, and machine learning. The developed approach was implemented using Python language. The testing environment was deployed for the experiments. The experiments proved that the developed tool allows the detection of security incidents and mapping them to the attack stages.

Besides, the authors compared the proposed tool with existing open solutions, namely, Splunk Enterprise Security, IBM QRadar SIEM, and HP ArcSight Security Intelligence. The comparison re-

■ ***Table 4.*** Comparison of the developed tool with known SIEMs

Tool	Dos_attack	Scan_attack	Shell_attack
Attack detected			
Developed tool	+	+	+
Other tools	+	+	+
Attack mapped			
Developed tool	T1499.001[1] T1499.002[2] T1499.003[3] T1499.004[4]	T1595.001[5] T1595.002[6]	T1505.001[7] T1505.002[8] T1505.003[9]
Other tools	–	–	–

[1] https://attack.mitre.org/techniques/T1499/001/
[2] https://attack.mitre.org/techniques/T1499/002/
[3] https://attack.mitre.org/techniques/T1499/003/
[4] https://attack.mitre.org/techniques/T1499/004/
[5] https://attack.mitre.org/techniques/T1595/001/
[6] https://attack.mitre.org/techniques/T1595/002/
[7] https://attack.mitre.org/techniques/T1505/001/
[8] https://attack.mitre.org/techniques/T1505/002/
[9] https://attack.mitre.org/techniques/T1505/003/

sults are given in Table 4. Existing tools as well as the developed tool can detect all the conducted attacks. But unlike existing tools that are not able to map the detected attacks to the MITRE ATT & CK techniques and tactics, the developed tool is also able to detect techniques and tactics corresponding to the detected incident according to the MITRE ATT & CK. Thus, $Res_{PA} \geq Res_{EA}$, and the goal of the research is accomplished.

There are some limitations of the approach. Thus, the event correlation stage requires the correlation rules. We used the Emerging Threats correlation rules. If the rule for the security incident doesn't exist, the proposed solution won't detect the security incident. The same limitation exists for the incident mapping functionality. We implement mapping to the MITRE ATT & CK tactics and techniques using the TAA (IOA) rules. If the rule for the MITRE ATT & CK tactics or techniques doesn't exist, the proposed solution won't map the detected security incident to the attack sequence. Besides, there are some performance limitations. Thus, for the attack graph generation and probability calculation within the security assessment the resource consuming traversal algorithms are used. As soon as the attack graph is generated in the static mode before the system operation, this is not a drawback. To solve the probability calculation challenge in the real time mode we limit the number of the processed graph nodes.

Detection of the attack stage requires additional time and resources as well. However, automation of the cyber incident analysis will allow for saving the resources in future. Thus, this is essential for prevention of the targeted multi-step attacks. Their detection at an early stage, further assessment, and correct forecasting of the attack goal allow avoid the attack's success and impact from its successful implementation. The proposed solution can be implemented to protect heterogeneous infrastructures from cyber attacks.

In further research, the authors plan to enhance the proposed approach and corresponding tool in the following aspects:

— extending covered cyber attack scenarios using more complex correlation rules for the detection of cyber security incidents;

— considering attack scenarios that are not included to the MITRE ATT & CK database, such as generating targeted attacks using artificial neural networks;

— conducting other types of attacks to map other types of cyber security incidents to the MITRE ATT & CK tactics and techniques;

— adding the technique for the prospective countermeasures selection to the developed approach.

References

1. Kotenko I., Fedorchenko A., Doynikova E. *Data Analytics for Security Management of Complex Heterogeneous Systems: Event Correlation and Security Assessment Tasks*. In: *Advances in Cyber Security Analytics and Decision Systems*. Eds. S. K. Shandilya, N. Wagner, A. K. Nagar. Springer International Publishing, Cham, 2020, pp. 79–116. https://doi.org/10.1007/978-3-030-19353-9_5. 455
2. Doynikova E., Novikova E., Gaifulina D., Kotenko I. Towards attacker attribution for risk analysis. *Proc. of the 15th Intern. Conf. "Risks and Security of Internet and Systems CRiSIS 2020"*. Springer-Verlag, Berlin, Heidelberg, 2020, pp. 347–353. https://doi.org/10.1007/978-3-030-68887-5_22
3. Kovačević I., Groš S., Slovenec K. Systematic review and quantitative comparison of cyberattack scenario detection and projection. *Electronics*, 2020, vol. 9, no. 10, pp. 1722.
4. Pavlov A., Voloshina N. Analysis of IDS alert correlation techniques for attacker group recognition in distributed systems. *Proc. of the 20th Intern. Conf. "Internet of Things, Smart Spaces and Next Generation Networks and Systems NEW2AN 2020", and 13th Conf. ruSMART 2020*. Springer-Verlag, Berlin, Heidelberg, 2020, pp. 32–42. https://doi.org/10.1007/978-3-030-65726-0_4

5. Bajtoš T., Sokol P., Mézešová M. *Multi-stage Cyber-attacks Detection in the Industrial Control Systems*. In: *Recent Developments on Industrial Control Systems Resilience*. Eds. E. Pricop, J. Fattahi, N. Dutta, M. Ibrahim. Springer, 2020, pp. 151–173.

6. Stroeh K., Mauro Madeira E. R., Goldenstein S. K. An approach to the correlation of security events based on machine learning techniques. *Journal of Internet Services and Application*s, 2013, vol. 4, no. 7. https://doi.org/10.1186/1869-0238-4-7

7. Khosravi M., Ladani B. T. Alerts correlation and causal analysis for APT based cyber attack detection. *IEEE Access*, 2020, vol. 8, pp. 162642–162656. doi:10.1109/ACCESS.2020.3021499

8. Kotenko I., Gaifulina D., Zelichenok I. Systematic literature review of security event correlation methods. *IEEE Access*, 2022, no. 10, pp. 43387–43420. https://doi.org/10.1109/ACCESS.2022.3168976

9. Kryukov R., Zima V., Fedorchenko E., Novikova E., Kotenko I. Mapping the security events to the MITRE ATT&CK attack patterns to forecast attack propagation (extended abstract). *Proc. of the 5th Intern. Workshop "Attacks and Defenses for the Internet-of-Things ADIoT 2022"*. Springer Nature Switzerland, Cham, 2022, pp. 165–176.

10. Gao P., Shao F., Liu X., Xiao X., Qin Z., Xu F., Mittal P., Kulkarni S. R., Song D. Enabling efficient cyber threat hunting with cyber threat intelligence. *Proc. of the 2021 IEEE 37th Intern. Conf. on Data Engineering (ICDE)*. IEEE Computer Society, 2021, pp. 193–204. https://doi.org/10.1109/ICDE51399.2021.00024

11. Kurniawan K., Ekelhart A., Kiesling E., Quirchmayr G., Tjoa A. M. KRYSTAL: Knowledge graph-based framework for tactical attack discovery in audit data. *Computers & Security*, 2022, vol. 121, pp. 102828. https://doi.org/10.1016/j.cose.2022.102828

12. Sadlek L., Čeleda P., Tovarňák D. Identification of attack paths using kill chain and attack graphs. *Proc. of the NOMS 2022-2022 IEEE/IFIP Network Operations and Management Symp*. IEEE, 2022, pp. 1–6. https://doi.org/10.1109/NOMS54207.2022.9789803

13. Xiong W., Legrand E., Åberg O., Lagerström R. Cyber security threat modeling based on the MITRE Enterprise ATT&CK Matrix. *Software and Systems Modeling*, 2022, vol. 21, pp. 157–177. https://doi.org/10.1007/s10270-021-00898-7

14. Ajmal A. B., Shah M. A., Maple C., Asghar M. N., Islam S. U. Offensive security: Towards proactive threat hunting via adversary emulation. *IEEE Access*, 2021, no. 9, pp. 126023–126033. https://doi.org/10.1109/ACCESS.2021.3104260

15. Choi S., Yun J. H., Min B. G. Probabilistic attack sequence generation and execution based on MITRE ATT&CK for ICS datasets. *Proc. of the Cyber Security Experimentation and Test Workshop CSET'21*. New York, USA, 2021, pp. 41–48. https://doi.org/10.1145/3474718.3474722

16. Elitzur A., Puzis, R., Zilberman P. Attack hypothesis generation. *Proc. of the 2019 European Intelligence and Security Informatics Conf. (EISIC 2019)*. Institute of Electrical and Electronics Engineers, 2019, pp. 40–47. https://doi.org/10.1109/EISIC49498.2019.9108886

17. Nisioti A., Loukas G., Laszka A., Panaousis E. Data-driven decision support for optimizing cyber forensic investigations. *IEEE Transactions on Information Forensics and Security*, 2021, vol. 16, pp. 2397–2412. https://doi.org/10.1109/TIFS.2021.3054966

18. Al-Shaer R., Spring J. M., Christou E. Learning the associations of MITRE ATT&CK adversarial techniques. *Proc. of the 2020 IEEE Conf. on Communications and Network Security (CNS)*, 2020, pp. 1–9. https://doi.org/10.1109/CNS48642.2020.9162207

19. Kim K., Shin Y., Lee J., Lee K. Automatically attributing mobile threat actors by vectorized ATT&CK Matrix and paired indicator. *Sensors*, 2021, vol. 21, iss. 19. https://doi.org/10.3390/s21196522

20. Poolsappasit N., Dewri R., Ray I. Dynamic security risk management using bayesian attack graphs. *IEEE Transactions on Dependable and Secure Computing*, 2012, vol. 9, iss. 1, pp. 61–74. https://doi.org/10.1109/TDSC.2011.34

УДК 004.056
doi:10.31799/1684-8853-2024-2-39-50
EDN: YXVAJI

Оценивание защищенности гетерогенных инфраструктур на основе графов атак с использованием баз данных NVD и MITRE ATT & CK

Р. О. Крюков[а], канд. техн. наук, преподаватель, orcid.org/0009-0008-3422-7234
Е. В. Федорченко[б], канд. техн. наук, старший научный сотрудник, orcid.org/0000-0001-6707-9153
И. В. Котенко[б], доктор техн. наук, профессор, orcid.org/0000-0001-6859-7120, ivkote@comsec.spb.ru
Е. С. Новикова[б], канд. техн. наук, доцент, orcid.org/0000-0003-2923-4954
В. М. Зима[а], канд. техн. наук, профессор, orcid.org/0009-0006-9412-4160
[а]Военно-космическая академия им. А. Ф. Можайского, Ждановская наб., 13, Санкт-Петербург, 197198, РФ
[б]Санкт-Петербургский Федеральный исследовательский центр РАН, 14-я линия В.О., 39, Санкт-Петербург, 199178, РФ

Введение: оценивание защищенности современных информационных систем является нетривиальной задачей. Такие системы объединяют различные объекты, «вещи», субъекты и связи между ними, при этом они постоянно меняются и генерируют большое количество событий. В результате постоянно меняется состояние защищенности системы. **Цель:** разработать подход к оценке защищенности гетерогенных информационных систем. **Результаты:** разработан подход к оцениванию защищенности, который включает сбор данных из различных открытых источников, предобработку журналов событий, обнаружение инцидентов безопасности, отображение инцидентов безопасности на узлы графа атак, оценивание и прогнозирование уровня защищенности и представление результатов. Новизна предложенного подхода заключается в разработанной методике отображения инцидентов на этапы целевых кибератак. Эта методика использует правила корреляции Emerging Threats для обнаружения инцидентов безопасности. Для отображения обнаруженных инцидентов безопасности на шаблоны атак из базы данных MITRE ATT & CK методика использует правила Targeted Attack Analyzer (Indicators of Attack), которые описывают инциденты безопасности (сигнатуры) с использованием языка Sigma. Методика позволяет отобразить обнаруженные события на граф атак и оценить и спрогнозировать целевые кибератаки. Для генерации графа атак предлагается использовать шаблоны атак из MITRE ATT & CK и уязвимости из National Vulnerability Database (Национальной базы данных уязвимостей). Предложенный подход реализован в рамках программного средства, написанного на языке Python. Для тестирования отображения обнаруженных инцидентов безопасности на известные шаблоны атак развернута тестовая среда. **Практическая значимость:** результаты исследования могут быть использованы при построении систем оценивания защищенности, которые направлены на повышение защищенности гетерогенных информационных систем от кибератак.

Ключевые слова — оценивание защищенности, инциденты кибербезопасности, корреляция событий, сигнатура, кибератака, граф атак, MITRE ATT & CK, National Vulnerability Database, анализатор целевых атак, индикаторы атаки, киберугроза.

Для цитирования: Kryukov R. O., Fedorchenko E. V., Kotenko I. V., Novikova E. S., Zima V. M. Security assessment based on attack graphs using NVD and MITRE ATT & CK database for heterogeneous infrastructures. *Информационно-управляющие системы*, 2024, № 2, с. 39–50. doi:10.31799/1684-8853-2024-2-39-50, EDN: YXVAJI

For citation: Kryukov R. O., Fedorchenko E. V., Kotenko I. V., Novikova E. S., Zima V. M. Security assessment based on attack graphs using NVD and MITRE ATT & CK database for heterogeneous infrastructures. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2024, no. 2, pp. 39–50. doi:10.31799/1684-8853-2024-2-39-50, EDN: YXVAJI

5-я Международная научно-техническая конференция «Современные сетевые технологии — MoNeTec-2024»

29–31 октября 2024 г., Москва, Россия
https://www.monetec.ru

Организаторы конференции

- Московский государственный университет имени М. В. Ломоносова, факультет вычислительной математики и кибернетики
- Центр прикладных исследований компьютерных сетей

Программный комитет

В программный комитет входят 38 ученых из четырех стран, из них 17 состоят в IEEE. Список членов программного комитета MoNeTec-2024 доступен на официальном сайте по ссылке https://monetec.ru/committee

Организационный комитет

Список членов организационного комитета MoNeTec-2024 доступен на официальном сайте по ссылке https://monetec.ru/organizing_committee/

Контакты организационного комитета:
- e-mail: info@monetec.ru
- тел: +7 (495) 9394671

Тематика и цель

5-я Международная научно-техническая конференция «Современные сетевые технологии» собирает представителей международного научного сообщества, исследовательских подразделений корпораций, стартапов, промышленности и бизнеса, институтов развития и органов государственной власти для обсуждения перспективных и актуальных технологий в сфере компьютерных сетей, виртуализации сетевых ресурсов и облачных вычислений, использования методов искусственного интеллекта.

Технологии передачи данных являются основой современной цивилизации. Области телекоммуникации вбирают в себя и постоянно порождают все новые и новые технологии, которые открывают новые возможности, повышают качество сервиса и безопасность в современных сетях. Технологии программного управления в сетях, виртуализации сервисов, периферийные облачные вычисления стали ключевыми элементами построения современных сетей передачи данных и информационных инфраструктур в целом. В настоящее время в мире (и в России в частности) начато их применение на практике. Однако творческая мысль не останавливается на достигнутом. Сегодня мы уже говорим о реконфигурируемых по требованию сетях (Intent Based Network), информационно-ориентированных сетях (Information Centric Network), контент-ориентированных сетях (Content Centric Network). Возникает много новых проблем и направлений для исследований.

На конференции планируются выступления с пленарными докладами ряда зарубежных и отечественных ученых по перспективным направлениям развития современных сетей передачи данных и их приложений. Программа конференции также предусматривает проведение нескольких школ по сетевым технологиям и применению отечественных решений по тематике конференции для молодых ученых, студентов старших курсов и аспирантов. Это будет способствовать расширению профессионального круга специалистов, способных поддерживать и развивать эти технологии и решения.

Направления работы MoNeTec-2024

- QoS control in data communication
- Resource management and control in cloud computing
- Edge computing

- Information security in SDN/cloud
- 5G/6G networks for wireless communication
- 6G radio access networks
- Coding theory applications in networking
- High-speed routing and switching
- Heterogeneous channel traffic modeling and analysis
- Large-scale network simulation: methods and tools
- Formal verification of network protocols and service
- AI-driven IoT sensing, interaction, and digitalization
- IIoT: Industrial Internet of Things
- Domain specific networks
- AI4net, AI for network and network for AI
- AIoT: Artificial Intelligence of Things
- Future networking

Программный комитет приветствует подачу докладов, посвященных применению методов искусственного интеллекта в указанных выше направлениях.

Подача докладов

Доклад должен представлять собой оригинальный, ранее не опубликованный результат. Информация о требованиях к докладам и процедуре подачи докладов размещена на сайте конференции https://www.monetec.ru

Материалы для публикации — доклады объемом до 12 страниц в формате pdf на английском языке — представляются через систему uConfy. Подробная информация о типах докладов представлена на сайте.

Для оформления статей необходимо использовать стандартный шаблон IEEE для материалов международных конференций (формат A4).

Для конференции запрошена техническая поддержка IEEE. Доклады на английском языке, успешно прошедшие отбор и представленные на конференции, будут поданы для публикации в библиотеке IEEE Xplore (индексация в Scopus).

Авторы могут подать доклад на русском языке. Такие доклады будут представлены на отдельной секции(ях) и опубликованы в сборнике трудов, индексируемом в РИНЦ.

По итогам выступлений авторам докладов может быть предложено доработать текст до полноформатной статьи, которая будет рекомендована для публикации в журналах из перечня ВАК и ядра РИНЦ.

Информация об оргвзносе для участников будет доступна на сайте конференции.

Стендовые доклады

Авторам докладов, отклоненных по итогам рецензирования, может быть предложено представить стендовый доклад. Докладчик предоставляет файл плаката; печать плаката (85×110 см) и размещение его на стенде выполняют организаторы конференции. Стендовые доклады **не** публикуются в сборнике трудов для IEEE Xplore, они будут опубликованы в сборнике, индексируемом в РИНЦ.

Школы по сетевым и облачным технологиям

Перед началом конференции планируется проведение нескольких школ по сетевым и облачным технологиям. Цель этих школ — познакомить слушателей с современными технологиями, показать их преимущества и возможности. Регистрация для участия в каждой школе будет открыта на сайте конференции. Количество мест в каждой из школ ограничено.

Важные даты

- Представление аннотаций (extended abstract) докладов: **до 1 мая 2024 г.**
- Результаты предварительного рецензирования: **до 15 мая 2024 г.**
- Представление докладов: **до 15 июня 2024 г.**
- Результаты рецензирования: **до 1 сентября 2024 г.**
- Предоставление финальной версии доклада, доработанного по результатам рецензирования: **до 20 сентября 2024 г.**
- Регистрация для участия в школе: **до 5 октября 2024 г.**
- Школы: **27–28 октября 2024 г.**
- Конференция: **29–31 октября 2024 г.**

Формат и место проведения

Формат конференции: смешанный (очный и дистанционный)

Место проведения: Московский государственный университет имени М. В. Ломоносова

Прошедшие конференции MoNeTec

Первая конференция MoNeTec-2014 (27–29 октября 2014 г.)

Место проведения: МГУ имени М. В. Ломоносова

Труды конференции: https://ieeexplore.ieee.org/xpl/conhome/8555058/proceeding

Вторая конференция MoNeTec-2018 (25–26 октября 2018 г.)

Место проведения: Сколтех (Москва)

Труды конференции: https://ieeexplore.ieee.org/xpl/conhome/8555058/proceeding

Третья конференция MoNeTec-2020 (27–29 октября 2020 г.)

Место проведения: online

Презентации и видеоконференции: https://monetec.ru/2020/reports

Труды конференции: https://ieeexplore.ieee.org/xpl/conhome/9257984/proceeding

Четвертая конференция MoNeTec-2022 (27–29 октября 2022 г.)

Место проведения: МТУСИ

Труды конференции: https://ieeexplore.ieee.org/xpl/conhome/9960711/proceeding

УВАЖАЕМЫЕ АВТОРЫ!

Научные базы данных, включая Scopus и Web of Science, обрабатывают данные автоматически. С одной стороны, это ускоряет процесс обработки данных, с другой — различия в транслитерации ФИО, неточные данные о месте работы, области научного знания и т. д. приводят к тому, что в базах оказывается несколько авторских страниц для одного и того же человека. В результате для всех по отдельности считаются индексы цитирования, что снижает рейтинг ученого.

Для идентификации авторов в сетях Thomson Reuters проводит регистрацию с присвоением уникального индекса (ID) для каждого из авторов научных публикаций.

Процедура получения ID бесплатна и очень проста, есть возможность провести регистрацию на 12 языках, включая русский (чтобы выбрать язык, кликните на зеленое поле вверху справа на стартовой странице): https://orcid.org

СВЕДЕНИЯ ОБ АВТОРАХ

БАЛОНИН Юрий Николаевич

Научный сотрудник кафедры вычислительных систем и сетей Санкт-Петербургского государственного университета аэрокосмического приборостроения.
В 2010 году окончил Санкт-Петербургский государственный университет аэрокосмического приборостроения по специальности «Вычислительные машины, комплексы, системы и сети».
Является автором 17 научных публикаций.
Область научных интересов — вычислительные методы, теория чисел.
Эл. адрес: yuraball@mail.ru

ВОСТРИКОВ Антон Александрович

Доцент кафедры вычислительных систем и сетей Санкт-Петербургского государственного университета аэрокосмического приборостроения.
В 2000 году окончил Санкт-Петербургский государственный университет аэрокосмического приборостроения по специальности «Вычислительные машины, комплексы, системы и сети».
В 2004 году защитил диссертацию на соискание ученой степени кандидата технических наук.
Является автором 45 научных публикаций и двух свидетельств о регистрации программного продукта.
Область научных интересов — распределенные и встраиваемые информационно-управляющие системы, обработка визуальной информации, оптико-информационные системы.
Эл. адрес: vostricov@mail.ru

ИНИВАТОВ Даниил Павлович

Студент бакалавриата Омского государственного технического университета.
Является автором 41 научной публикации.
Область научных интересов — искусственный интеллект и машинное обучение.
Эл. адрес: daniilini@mail.ru

ВАСИЛЬЕВ Владимир Иванович

Профессор кафедры вычислительной техники и защиты информации Уфимского университета науки и технологий.
В 1970 году окончил Уфимский авиационный институт по специальности «Промышленная электроника».
В 1990 году защитил диссертацию на соискание ученой степени доктора технических наук.
Является автором более 450 научных публикаций.
Область научных интересов — проектирование и исследование многоуровневых систем управления сложными техническими объектами, интеллектуальных систем контроля, мониторинга и обеспечения информационной безопасности объектов критической информационной инфраструктуры.
Эл. адрес: vas0015@yandex.ru

ЗИМА Владимир Михайлович

Профессор кафедры систем сбора и обработки информации Военно-космической академии им. А. Ф. Можайского, Санкт-Петербург.
В 1988 году окончил Военный инженерно-космический институт им. А. Ф. Можайского по специальности «Электронные вычислительные машины».
В 1993 году защитил диссертацию на соискание ученой степени кандидата технических наук.
Является автором более 100 научных публикаций и двух патентов на изобретения.
Область научных интересов — разработка, анализ и совершенствование систем и средств информационно-компьютерной безопасности.
Эл. адрес: vladimir_zima@mail.ru

КОТЕНКО Игорь Витальевич

Профессор, главный научный сотрудник, заведующий лабораторией проблем компьютерной безопасности Санкт-Петербургского института информатики и автоматизации РАН.
В 1983 году окончил Военно-космическую академию им. А. Ф. Можайского по специальности «Математическое обеспечение автоматизированных систем управления», в 1987 году — Военную академию связи по специальности «Инженерная автоматизированных систем управления».
В 1999 году защитил диссертацию на соискание ученой степени доктора технических наук.
Является автором более 500 научных публикаций.
Область научных интересов — безопасность компьютерных сетей, обнаружение компьютерных атак, межсетевые экраны и др.
Эл. адрес: ivkote@comsec.spb.ru

КРЮКОВ Роман Олегович

Преподаватель кафедры систем сбора и обработки информации Военно-космической академии им. А. Ф. Можайского, Санкт-Петербург.
В 2013 году окончил Военно-космическую академию им. А. Ф. Можайского по специальности «Вычислительные машины, комплексы, системы и сети».
В 2020 году защитил диссертацию на соискание ученой степени кандидата технических наук.
Является автором десяти научных публикаций.
Область научных интересов — теория игр, методы принятия решений в условиях неопределенности, системы информационной безопасности.
Эл. адрес: roman682@yandex.ru

ЛЕ Туан Нгуен Хой

Студент, ассистент исследователя в группе по науке о данных на факультете информационных технологий Университета науки и технологий, Университет Дананга, Вьетнам.
Область научных интересов — взаимодействие человека с компьютером, искусственный интеллект и анализ данных.
Эл. адрес:
102210359@ sv1.dut.udn.vn

НГУЕН Ван Зунг

Студент, ассистент исследователя в группе по науке о данных на факультете информационных технологий Университета науки и технологий, Университет Дананга, Вьетнам.
Область научных интересов — методы анализа данных, искусственный интеллект и обработка изображений.
Эл. адрес:
102210356@ sv1.dut.udn.vn

КУРТЯНИК Даниил Владимирович

Старший преподаватель кафедры вычислительных систем и сетей Санкт-Петербургского государственного университета аэрокосмического приборостроения.
В 2010 году окончил Самарский государственный аэрокосмический университет им. академика С. П. Королёва по специальности «Механика».
Является автором более 20 научных публикаций.
Область научных интересов — вычислительная математика, численный анализ и ортогональные преобразования.
Эл. адрес: dvk88@yandex.ru

ЛОЖНИКОВ Павел Сергеевич

Заведующий кафедрой комплексной защиты информации Омского государственного технического университета.
В 2000 году окончил Омский государственный технический университет по специальности «Автоматизированные системы обработки информации и управления».
В 2005 году защитил диссертацию на соискание ученой степени кандидата технических наук.
Является автором более 100 научных публикаций и четырех патентов на изобретения.
Область научных интересов — искусственный интеллект, информационные технологии, информационная безопасность, распознавание образов.
Эл. адрес: lozhnikov@gmail.com

НОВИКОВА Евгения Сергеевна

Доцент кафедры информационных систем Санкт-Петербургского государственного электротехнического университета «ЛЭТИ», старший научный сотрудник лаборатории проблем компьютерной безопасности Санкт-Петербургского института информатики и автоматизации РАН.
В 2007 году окончила университет «ЛЭТИ» по специальности «Компьютерная безопасность».
В 2010 году защитила диссертацию на соискание ученой степени кандидата технических наук.
Является автором более 150 научных публикаций и трех патентов на изобретения.
Область научных интересов — компьютерная безопасность, применение методов машинного обучения для выявления аномалий в киберфизических системах и др.
Эл. адрес: novikova@comsec.spb.ru

СВЕДЕНИЯ ОБ АВТОРАХ

РЫЖОВ Константин Юрьевич

Аспирант Института информационных технологий и программирования Санкт-Петербургского государственного университета аэрокосмического приборостроения.
В 2018 году окончил магистратуру Санкт-Петербургского государственного университета аэрокосмического приборостроения по специальности «Информатика и вычислительная техника».
Является автором пяти научных публикаций.
Область научных интересов — большие данные, искусственный интеллект, информационная безопасность, квантовые технологии и др.
Эл. адрес:
Konstantin.r02.27@gmail.com

СУЛАВКО Алексей Евгеньевич

Доцент кафедры комплексной защиты информации Омского государственного технического университета.
В 2009 году окончил Сибирскую государственную автомобильно-дорожную академию по специальности «Комплексное обеспечение информационной безопасности автоматизированных систем».
В 2014 году защитил диссертацию на соискание ученой степени кандидата технических наук.
Является автором более 130 научных публикаций и одного патента на изобретение.
Область научных интересов — распознавание образов, машинное обучение, биометрия, искусственный интеллект, защита информации, искусственные нейронные сети.
Эл. адрес: sulavich@mail.ru

ФАМ Конг Тханг

Преподаватель факультета информационных технологий Данангского университета науки и технологий, Дананг, Вьетнам.
В 2013 году окончил Тульский государственный университет по специальности «Вычислительные машины, комплексы, системы и сети».
В 2016 году защитил диссертацию на соискание ученой степени кандидата технических наук в Тульском государственном университете.
Является автором 30 научных публикаций.
Область научных интересов — обработка изображений, машинное обучение, наука о данных.
Эл. адрес: pcthang@dut.udn.vn

СЕРГЕЕВ Александр Михайлович

Доцент кафедры вычислительных систем и сетей Санкт-Петербургского государственного университета аэрокосмического приборостроения.
В 2004 году окончил Санкт-Петербургский государственный университет аэрокосмического приборостроения по специальности «Вычислительные машины, комплексы, системы и сети».
В 2020 году защитил диссертацию на соискание ученой степени кандидата технических наук.
Является автором 38 научных публикаций.
Область научных интересов — численные методы, теория вычислительных процессов, проектирование специализированных процессоров.
Эл. адрес: asklab@mail.ru

ФАМ Зуи Тин

Студент, ассистент исследователя в группе по науке о данных на факультете информационных технологий Университета науки и технологий, Университет Даланга, Вьетнам.
Область научных интересов — методы анализа данных, искусственный интеллект и обработка изображений.
Эл. адрес:
102210380@sv1.dut.udn.vn

ФЕДОРЧЕНКО Елена Владимировна

Старший научный сотрудник лаборатории проблем компьютерной безопасности Санкт-Петербургского института информатики и автоматизации РАН.
В 2009 году окончила Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» по специальности «Компьютерная безопасность».
В 2017 году защитила диссертацию на соискание ученой степени кандидата технических наук.
Является автором более 100 научных публикаций
Область научных интересов — информационная безопасность и конфиденциальность персональных данных, анализ и оценка информационной безопасности и конфиденциальности персональных данных и др.
Эл. адрес:
doynikova@comsec.spb.ru

ЧАН
Тхи Тху Тхао

Преподаватель факультета статистики и информатики Экономического университета, Данангский университет, Дананг, Вьетнам.
В 2018 году окончила магистратуру Тульского государственного университета по специальности «Прикладная математика и информатика».
Является автором 15 научных публикаций.
Область научных интересов — обработка изображений, машинное обучение.
Эл. адрес: thaotran@due.udn.vn

ПАМЯТКА ДЛЯ АВТОРОВ

Поступающие в редакцию статьи проходят обязательное рецензирование.

При наличии положительной рецензии статья рассматривается редакционной коллегией. Принятая в печать статья направляется автору для согласования редакторских правок. После согласования автор представляет в редакцию окончательный вариант текста статьи.

Процедуры согласования текста статьи могут осуществляться как непосредственно в редакции, так и по e-mail (ius.spb@gmail.com).

При отклонении статьи редакция представляет автору мотивированное заключение и рецензию, при необходимости доработать статью — рецензию.

Редакция журнала напоминает, что ответственность за достоверность и точность рекламных материалов несут рекламодатели.

Уважаемые авторы!

При подготовке рукописей статей необходимо руководствоваться следующими рекомендациями.

Статьи должны содержать изложение новых научных результатов. Название статьи должно быть кратким, но информативным. В названии недопустимо использование сокращений, кроме самых общепринятых (РАН, РФ, САПР и т. п.).

Текст рукописи должен быть оригинальным, а цитирование и самоцитирование корректно оформлено.

Объем статьи (текст, таблицы, иллюстрации и библиография) не должен превышать эквивалента в 20 страниц, напечатанных на бумаге формата А4 на одной стороне через 1,5 интервала Word шрифтом Times New Roman размером 13, поля не менее двух сантиметров.

Обязательными элементами оформления статьи являются: индекс УДК, заглавие, инициалы и фамилия автора (авторов), ученая степень, звание (при отсутствии — должность), полное название организации, аннотация и ключевые слова на русском и английском языках, ORCID и электронный адрес одного из авторов. При написании аннотации не используйте аббревиатур и не делайте ссылок на источники в списке литературы. Предоставляйте подрисуночные подписи и названия таблиц на русском и английском языках.

Статьи авторов, не имеющих ученой степени, рекомендуется публиковать в соавторстве с научным руководителем, наличие подписи научного руководителя на рукописи обязательно; в случае самостоятельной публикации обязательно предоставляйте заверенную по месту работы рекомендацию научного руководителя с указанием его фамилии, имени, отчества, места работы, должности, ученого звания, ученой степени.

Простые **формулы** набирайте в Word, сложные с помощью редактора Mathtype или Equation. Для набора одной формулы не используйте два редактора; при наборе формул в формульном редакторе знаки препинания, ограничивающие формулу, набирайте вместе с формулой; для установки размера шрифта в Mathtype никогда не пользуйтесь вкладкой Other, Smaller, Larger, используйте заводские установки редактора, не подгоняйте размер символов в формулах под размер шрифта в тексте статьи, не растягивайте и не сжимайте мышью формулы, вставленные в текст; пробелы в формуле ставьте только после запятых при перечислении с помощью Ctrl+Shift+Space (пробел); не отделяйте пробелами знаки: + = – ×, а также пространство внутри скобок; для выделения греческих символов в Mathtype полужирным начертанием используйте Style → Other → bold.

Для набора формул в Word никогда не используйте вкладки: «Уравнение», «Конструктор», «Формула» (на верхней панели: «Вставка» — «Уравнение»), так как этот ресурс предназначен только для внутреннего использования в Word и не поддерживается программами, предназначенными для изготовления оригинал-макета журнала.

При наборе символов в тексте помните, что символы, обозначаемые латинскими буквами, набираются светлым курсивом, русскими и греческими — светлым прямым, векторы и матрицы — прямым полужирным шрифтом.

Подробнее см. http://i-us.ru/index.php/ius/author-guide

Иллюстрации:

— рисунки, графики, диаграммы, блок-схемы предоставляйте в виде отдельных исходных файлов, поддающихся редактированию, используя векторные программы: Visio (*.vsd, *.vsdx); Adobe Illustrator (*.ai); Coreldraw (*.cdr, версия не выше 15); Excel (*.xls); Word (*.docx); AutoCad, Matlab (экспорт в PDF, EPS, SVG, WMF, EMF); Компас (экспорт в PDF); веб-портал DRAW.IO (экспорт в PDF); Inkscape (экспорт в PDF);

— фото и растровые — в формате *.tif, *.png с максимальным разрешением (не менее 300 pixels/inch).

Наличие подрисуночных подписей и названий таблиц на русском и английском языках обязательно (желательно не повторяющих дословно комментарии к рисункам в тексте статьи).

В редакцию предоставляются:

— сведения об авторе (фамилия, имя, отчество, место работы, должность, ученое звание, учебное заведение и год его окончания, ученая степень и год защиты диссертации, область научных интересов, количество научных публикаций, домашний и служебный адреса и телефоны, e-mail), фото авторов: анфас, в темной одежде на белом фоне, должны быть видны плечи и грудь, высокая степень четкости изображения без теней и отблесков на лице, фото можно представить в электронном виде в формате *.tif, *.png, *.jpg с максимальным разрешением — не менее 300 pixels/inch при минимальном размере фото 40×55 мм;

— экспертное заключение;

— экспортное заключение.

Список литературы составляется по порядку ссылок в тексте и оформляется следующим образом:

— для книг и сборников — фамилия и инициалы авторов, полное название книги (сборника), город, издательство, год, общее количество страниц, doi;

— для журнальных статей — фамилия и инициалы авторов, полное название статьи, название журнала, год издания, номер журнала, номера страниц, doi;

— ссылки на иностранную литературу следует давать на языке оригинала без сокращений;

— при использовании web-материалов указывайте адрес сайта и дату обращения.

Список литературы оформляйте двумя отдельными блоками по образцам lit.dot на сайте журнала (http://i-us.ru/paperrules): Литература и References.

Более подробно правила подготовки текста с образцами изложены на нашем сайте в разделе «Руководство для авторов» – http://i-us.ru/index.php/ius/author-guide.

Контакты

Куда: 190000, г. Санкт-Петербург, ул. Большая Морская, д. 67, лит. А, ГУАП, РИЦ
Кому: Редакция журнала «Информационно-управляющие системы»
Тел.: (812) 494-70-02
Эл. почта: ius.spb@gmail.com
Сайт: www.i-us.ru