ОТЗЫВ

официального оппонента

доктора технических наук, профессора, заслуженного деятеля науки Российской Федерации Котенко Игоря Витальевича на диссертацию Панфиловой Ирины Евгеньевны на тему «Модели и алгоритмы нейросетевой биометрической аутентификации в защищенном режиме исполнения», представленную на соискание ученой степени кандидата технических наук по специальности

2.3.6. Методы и системы защиты информации, информационная безопасность

Актуальность темы диссертации

В условиях стремительного внедрения технологий искусственного интеллекта (ИИ) в системы распознавания по лицу важнейшим аспектом становится безопасность обработки биометрических данных. Данный способ, как один из наиболее распространенных методов идентификации, приобретает все большую популярность благодаря своему удобству и оперативности. Однако этот метод сталкивается с серьезными угрозами, такими как спуфинг, при котором злоумышленники используют фотографии или маски для обхода системы, а также атаки извлечения знаний, направленные на компрометацию алгоритмов. Кроме того, утечка биометрической информации может привести к серьезным последствиям для пользователей, включая возможность несанкционированного доступа к защищенным объектам. Эти вызовы подчеркивают необходимость создания эффективных механизмов защиты, обеспечивающих конфиденциальность и целостность пользовательской информации.

В этой связи нейросетевые преобразователи «биометрия-код» (НПБК) выступают как решение, обеспечивающее безопасность биометрических систем, в том числе, спроектированных на базе нейронных сетей. Их способность связывать биометрические данные с криптографическими ключами позволяет существенно уменьшить риски, связанные с компрометацией личной информации. Тем не менее, остаются нерешенные задачи, связанные с улучшением устойчивости таких систем к деструктивным воздействиям. Исследование методов защиты нейросетевой биометрической аутентификации по лицу с использованием НПБК становится ключевым направлением, способствующим повышению надежности и защищенности биометрических технологий в современных условиях.

Таким образом, можно сделать вывод, что диссертация Панфиловой И.Е., посвященная новому варианту защищенного исполнения нейросетевых алгоритмов

биометрической аутентификации по лицу на основе преобразователей «биометрия-код», является актуальной.

Оценка структуры и содержания работы

Диссертация состоит из введения, четырех глав, заключения, списка литературы и приложений. Диссертационное исследование изложено на 166 страницах и содержит 28 рисунков, 15 таблиц, 2 приложения. Список использованных источников содержит 195 наименований.

Во введении обосновывается актуальность темы диссертации, определены цель и задачи исследования, сформулированы положения, выносимые на защиту, научная новизна, а также практическая и теоретическая значимость полученных результатов.

Первая глава посвящена анализу проблемы защищенного исполнения ИИ в задачах биометрической аутентификации субъектов. Выделяются три направления защиты: биокриптографические системы (БКС), отменяемая биометрия и гомоморфное шифрование, с акцентом на преимущества БКС. Основные направления развития БКС включают нечеткие экстракторы и нейросетевые преобразователи «биометрия-код» (НПБК). Проведенный анализ показывает преимущество НПБК перед нечеткими экстракторами и выявляет недостатки существующих реализаций, таких как классические НПБК и НПБК на базе корреляционных нейронов, подчеркивая необходимость их улучшения в контексте лицевой биометрии.

Во второй главе разработана концепция защищенной биометрической аутентификации по лицу с использованием нейросетевого преобразователя «биометрия-код», направленная на защиту от спуфинг-атак. Концепция включает два независимых блока, один из которых выполняет аутентификацию посредством связывания биометрического образа лица с криптографическим ключом, а другой отвечает за обнаружение спуфинг-атак. Параметры, используемые для аутентификации, защищены с помощью наложенной гаммы, представляющей ключ НПБК, что предотвращает раскрытие данных.

В третьей главе предложена модель нейросетевого преобразователя «биометрия-код» (НПБК) на основе тригонометрических нейронов, обеспечивающая защищенный режим исполнения для классификации биометрических образов в рамках систем доверенного ИИ. Модель использует две альтернативные меры близости в подпространстве пар признаков, что позволяет значительно повысить точность классификации и увеличивает длину криптографического ключа. Экспериментальная оценка показала эффективность предложенной модели, обеспечившей более низкие значения EER на

тестовых наборах данных по сравнению с другими реализациями биометрических криптосистем.

В четвёртой главе представлена структура системы защищённой биометрической аутентификации. В основе структуры лежит способ построения механизма защиты нейросетевого контейнера, позволяющий защищать данные пользовательского НПБК. Система на основе предложенной структуры реализована в качестве программы и протестирована на базе разработанной совместно с автором среды управления жизненным циклом ИИ «AIC ModelOps Platform».

В заключении выделены основные результаты, полученные в диссертации.

Степень обоснованности научных положений, выводов и рекомендаций, сформулированных в диссертации

Обоснованность научных положений и выводов, представленных в диссертационном исследовании, подтверждается опубликованными материалами исследований работы, включающими в себя 6 статей в профильных научных журналах, входящих в Перечень рецензируемых научных изданий, рекомендованных ВАК, и 4 статьи в других изданиях.

Диссертация включает в себя достаточное количество иллюстраций и таблиц, необходимых для полного понимания результатов проведенных исследований. Автореферат адекватно отражает содержание диссертации, а также ключевые выводы и результаты, представленные в работе.

Полученные результаты соответствуют заявленным автором пунктам паспорта специальности «2.3.6. Методы и системы защиты информации, информационная безопасность».

Достоверность полученных результатов подтверждается результатами проведенных компьютерных экспериментов, государственной регистрацией программ для ЭВМ, а также успешным внедрением разработанной системы в образовательные и бизнес процессы. Основные результаты диссертационного исследования прошли апробацию на научных конференциях различного уровня.

Научная новизна полученных результатов

К новым научным результатам, полученным в диссертационной работе, относятся:

1. Концепция защищенной биометрической аутентификации по лицу, отличающаяся применением механизма защищенного нейросетевого контейнера (ЗНК) для безопасного взаимодействия блока аутентификации на основе пользовательского НПБК и блока обнаружения спуфинг атак на основе НПБК. Концепция позволяет обеспечивать устойчивость процедуры аутентификации к атакам на биометрическое предъявление

(спуфинг атакам), а также защиту таблиц нейросетевых функционалов пользовательского НПБК.

2. Модель тригонометрического нейрона и основанная на ней модель нейросетевого преобразователя, отличающиеся применением новой меры оценки расстояния между образами субъектов в подпространстве пар признаков и обеспечивающих защиту образов лиц. Предложенные модели обеспечивает защиту знаний НПБК от компрометации, так как не используют параметры распределений и/или характеристики образов легитимных пользователей.

3. Алгоритм калибровки нейросетевых преобразователей «биометрия-код» и алгоритм автоматического обучения НПБК, отличающиеся организацией такого совместного функционирования, при котором возможно быстрое и робастное обучение нейросетевых преобразователей «биометрия-код» на малых выборках образов лиц.

4. Структура системы защищенной биометрической аутентификации по лицу, отличающаяся наличием независимых блоков извлечения признаков, обучения нейросетевых преобразователей и аутентификации, а также применением нового варианта исполнения механизма защиты нейросетевого контейнера. Разработанная структура позволяет повысить защищенность процедуры биометрической аутентификации по лицу на основе в отношении спуфинг атак, а также атак извлечения знаний НПБК и компрометации биометрических образов лиц.

Теоретическая и практическая значимость результатов, полученных автором диссертационной работы

Теоретическая значимость результатов диссертационной работы заключается в предложенных моделях и алгоритмах обучения нейросетевого преобразователя «биометрия-код» (НПБК), работающего со слабо коррелированными признаками лица. Новый математический аппарат НПБК позволяет продуцировать длинный криптографический ключ, надежно защищающий биометрические образы от компрометации.

Практическая значимость полученных результатов состоит в разработке системы защищенной биометрической аутентификации по лицу, основанной на предложенных в работе концепции, моделях и алгоритмах. Полученные результаты работы системы, реализованной и протестированной посредствам специального программного обеспечения, также прошли практическую апробацию, подтвержденную актами о внедрении.

Замечания по работе

1. В исследовании представлено ограниченное количество ссылок на работы, позволяющие сравнить полученные результаты по применению НПБК в качестве

классификатора спуфинг атак с предыдущими достижениями на тех же наборах данных, в связи с чем, для оценки точности его работы использовались результаты, полученные на других наборах данных. Необходимо уточнить, как различия в структуре и характеристиках этих наборов могли повлиять на результаты сравнения, особенно с учетом специфики атак и устойчивости предложенной модели.

2. Не приведено четкого обоснования применения НПБК как метода определения спуфинг атак, а также объяснения причин повышения надежности детекции спуфинг атак с помощью НПБК.

3. Из материалов исследования не ясно, каким образом функционал тригонометрического нивелирования учитывает корреляционную зависимость признаков, и за счет чего данная мера близости показывает лучшие результаты на слабо коррелированных данных.

4. В рамках диссертационного исследования не проведено тестирование нейросетевого преобразователя «биометрия-код» на предмет устойчивости к спуфинг атакам, характеризующимся высокой степенью правдоподобия (так как набор данных CelebA-Spoof не включает в себя такой спуфинг, как, например, силиконовые маски). Какова ожидаемая эффективность НПБК против таких атак?

5. В алгоритме калибровки НПБК, описанном в третьей главе, мета-признаки ранжируются и делятся на 3 равные части, однако не раскрыто, предполагается ли при этом, что мета-признаки обладают однородностью или иными специфическими свойствами, делающими данный подход оптимальным. Также не уточняется, как ранжирование и равномерное деление сказываются на точности и устойчивости алгоритма при вариативности данных.

6. В главах 2 и 3 внимание сосредоточено на исследовании применения нейросетевого преобразователя «биометрия-код» для задач обнаружения спуфинг атак и аутентификации пользователей соответственно, тогда как глава 4 описывает разработку целостной системы на основе этих решений. Было бы полезно дополнить разделы 2.5 и 3.5 промежуточными выводами, более чётко указывающими, как разработанные концепция и модели интегрируются в общую архитектуру системы.

В целом, указанные замечания не снижают ценности полученных в диссертационной работе результатов и не влияют на общую положительную оценку диссертации.

Заключение

Диссертация Панфиловой И.Е., представленная на соискание ученой степени кандидата технических наук, является законченной научно-квалификационной работой, посвященной решению актуальной задачи повышения защищенности процедуры

нейросетевой биометрической аутентификации по лицу на основе нейросетевого преобразователя «биометрия-код». Результаты диссертационного исследования обладают научной новизной, теоретической и практической значимостью.

Диссертационная работа соответствует требованиям п. 9 «Положения о присуждении ученых степеней», утвержденного Постановлением Правительства Российской федерации от 24 сентября 2013 года №842 (с изменениями и дополнениями), а ее автор, Панфилова И.Е., заслуживает присуждения учёной степени кандидата технических наук по специальности «2.3.6. Методы и системы защиты информации, информационная безопасность».

Официальный оппонент:
Доктор технических наук, профессор,
заслуженный деятель науки Российской Федерации,
главный научный сотрудник лаборатории
проблем компьютерной безопасности,
Федеральное государственное бюджетное
учреждение науки «Санкт-Петербургский
Федеральный исследовательский центр
Российской академии наук»

«12» ноября 2024 г. Котенко Игорь Витальевич

Докторская диссертация защищена по специальностям:
20.01.09 - "Военные системы управления и связи"
20.02.13 - "Информатика и компьютерные технологии в военном деле"

Даю согласие на обработку персональных данных.

Адрес места основной работы: 199178, Россия, Санкт-Петербург, 14 линия, дом 39
Рабочий телефон: +7 (812) 328-34-11
Адрес эл. почты: ivkote@comsec.spb.ru

Подпись руки Котенко И.В. заверяю
Заместитель начальника отдела кадров СПб ФИЦ РАН
И.В. Невмержицкая
«12» ноября 2024 г.