ОТЗЫВ

официального оппонента

доктора физико-математических наук, доцента Исмагиловой Альбины Сабирьяновны на диссертационную работу 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

Актуальность диссертационного исследования, проведенного Панфиловой Ириной Евгеньевной, заключается в решении одной из ключевых проблем современной биометрической аутентификации – обеспечении конфиденциальности биометрических данных. Несмотря на существование ряда ранее разработанных стандартов, регламентирующих создание надежных систем биометрической аутентификации, остаются нерешенные вопросы, препятствующие широкому и безопасному применению нейросетевых биометрических систем, включая те, что функционируют на основе анализа изображений лиц человека.

Одной из существенных проблем является недостаточная длина криптографического ключа, который ассоциируется с биометрическим образом в защищенных системах аутентификации. Короткие ключи подвержены атакам методом перебора, что может привести к компрометации системы. Кроме того, необходимо учитывать общую уязвимость защищенных биометрических систем к атакам на биометрическое предъявление, в ходе которых злоумышленники могут подделывать или воспроизводить биометрические данные с целью осуществления несанкционированного доступа.

В контексте указанных проблем исследование Панфиловой Ирины Евгеньевны приобретает особую значимость. Основные положения работы сосредоточены на разработке моделей и алгоритмов, направленных на снижение вероятности ошибок аутентификации, при этом повышая длину криптографических ключей и снижая уязвимость системы биометрической аутентификации по лицу, основанной на нейронных сетях, к спуфинг-атакам. В качестве основы исследования рассматривается модификация защищенного исполнения нейросетевых алгоритмов биометрической аутентификации, использующая нейросетевые преобразователи «биометрия-код» (НПБК), что значительно повышает устойчивость систем аутентификации по лицу к внешним деструктивным воздействиям.

Оценка структуры и содержания работы

Работа состоит из введения, четырех глав, заключения, списка сокращений, списка литературы и приложений. Общее количество страниц – 166, включая 28 рисунков, 15 таблиц и 2 приложения. Список использованных источников состоит из 195 наименований.

Во введении сформулированы цель и задачи диссертационного исследования, обоснована его актуальность, а также выделены компоненты научной новизны работы и практическая значимость полученных результатов.

Первая глава посвящена анализу современных исследований в области защищенного исполнения искусственного интеллекта для биометрической аутентификации, с акцентом на проблемы уязвимости к атакам, включая спуфинг. Рассматриваются методы защиты биометрических данных, такие как биокриптографические системы (БКС), отменяемая биометрия и гомоморфное шифрование, с акцентом на преимущества БКС. Важным направлением исследования выделяются НПБК и необходимость устранения их недостатков в контексте лицевой биометрии.

Во второй главе разработана концепция защищенной биометрической аутентификации по лицу, основанная на нейросетевом преобразователе «биометрия-код», который демонстрирует устойчивость к спуфинг-атакам. В данной главе подчеркивается, что предложенный подход не только защищает от атак на биометрическое предъявление, но и обеспечивает безопасность параметров пользовательского НПБК. Описана процедура защиты этих параметров через их сокрытие с использованием ключа НПБК для эффективного обнаружения атак на биометрическое предъявление.

В третьей главе представлен процесс разработки и обучения нейросетевого преобразователя «биометрия-код», предназначенного для безопасной биометрической аутентификации на основе лицевых изображений. Разработан новый математический аппарат для построения нейронов, основанный на тригонометрической мере оценки расстояний между образами «Своего» и «Чужих». Подчеркнуто, что основное отличие предложенной модели заключается в том, что тригонометрическая мера оценки расстояний позволяет учитывать не только линейные различия между биометрическими признаками, но и их взаимные угловые характеристики, что способствует повышению устойчивости системы к атакующим воздействиям.

В четвертой главе представлена структура системы защищенной биометрической аутентификации, основанная на предложенных концепциях, моделях и алгоритмах. Описана процедура реализации системы с использованием языка программирования Python, а также проведено тестирование с применением специального разработанного программного обеспечения. Приведены результаты тестирования, подтверждающие эффективность предложенной системы.

В заключении приведены основные результаты диссертационного исследования.

Приложения содержат акты о внедрении результатов работы, а также свидетельства о государственной регистрации программ для ЭВМ.

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

Основные положения и выводы, представленные в данной работе, обладают полной обоснованностью, что подтверждается корректным применением методов исследования, четкой формулировкой целей и задач, а также соответствующими публикациями, основанными на материалах диссертации. Диссертация отличается логичной и последовательной структурой и сопровождается достаточным количеством иллюстраций и таблиц, которые наглядно демонстрируют ключевые результаты исследования. Содержание автореферата полностью отражает основные идеи и выводы, изложенные в диссертационной работе. Полученные результаты соответствуют заявленным автором пунктам паспорта научной специальности 2.3.6 Методы и системы защиты информации; информационная безопасность.

Достоверность полученных результатов подтверждается результатами сравнительного анализа имеющихся исходных данных и данных, полученных в процессе математического моделирования, а также апробацией полученных результатов при решении практических задач. Все положения, выносимые на защиту, обоснованы теоретически и не противоречат известным принципам теории и практики информационной безопасности. Все результаты были получены на основе численного и компьютерного моделирования, что свидетельствует о их достоверности.

Научная новизна полученных результатов

Наиболее существенные новые научные результаты, полученные в диссертационной работе, состоят в разработке научно-обоснованного концептуального подхода, моделей и алгоритмов решения поставленных задач. К новым научным результатам, полученным в диссертационном исследовании следует отнести следующие:

1. Концепция защищенной биометрической аутентификации на основе лицевого распознавания, характеризующаяся использованием механизма защищенного нейросетевого контейнера (ЗНК) для обеспечения безопасного взаимодействия между

блоком аутентификации, основанным на пользовательском НПБК, и блоком обнаружения спуфинг-атак, реализованным в виде классификатора, различающего реальные и поддельные изображения лиц. Данная концепция обеспечивает устойчивость процедуры аутентификации к атакам, направленным на биометрическое предъявление (спуфинг-атаки), а также дополнительную защиту таблиц нейросетевых функционалов пользовательского НПБК.

2. Модель тригонометрического нейрона и основанная на ней модель НПБК отличаются применением новой тригонометрической меры для оценки расстояния между образами субъектов в подпространстве пар признаков, что обеспечивает защиту лицевых изображений от компрометации путем генерации длинного криптографического ключа при высокой точности классификации. Предложенные модели не используют параметры распределений и/или характеристики образов легитимных пользователей, что способствует защите знаний НПБК от компрометации.

3. Алгоритм калибровки нейросетевых преобразователей «биометрия-код» и алгоритм обучения НПБК, основанные на тригонометрических нейронах, характеризуются использованием дополнительной информации, полученной путем оценки набора биометрических образов лиц, не участвующего в процессе обучения. Это позволяет осуществлять быстрое и устойчивое обучение пользовательских НПБК на ограниченных выборках лицевых изображений.

4. Структура системы защищенной биометрической аутентификации на основе лицевого распознавания отличается наличием независимых блоков извлечения признаков, обучения нейросетевых преобразователей и аутентификации, а также использованием варианта реализации ЗНК, при котором в режиме обучения ключом НПБК для обнаружения спуфинг-атак обеспечивается защита структуры пользовательского НПБК, а обратный процесс происходит во время аутентификации. Разработанная структура позволяет значительно повысить защищенность процедуры биометрической аутентификации личности по лицу на основе НПБК относительно спуфинг-атак, атак на извлечение знаний НПБК и компрометации биометрических изображений лиц.

Теоретическая и практическая значимость результатов, полученных автором диссертационной работы

Теоретическая значимость результатов диссертационной работы заключается в предложенной концепции, моделях и алгоритмах обучения. Разработанный математический аппарат нейросетевого преобразователя «биометрия-код» обеспечивает комплексный подход к решению проблемы повышения защищенности нейросетевой биометрической аутентификации, позволяя эффективно работать со слабо коррелированными признаками лицевых изображений человека.

Практическая значимость результатов, представленных автором диссертации, заключается в разработке системы защищенной биометрической аутентификации на основе лицевого распознавания и ее программной реализации. Полученные результаты были подвергнуты практической апробации, что подтверждается соответствующими актами о внедрении.

Замечания по работе

1. Утверждение о слабой корреляции между признаками, извлекаемыми из изображений лиц, не представлено в достаточной степени обоснованным. Целесообразно было бы указать, какие конкретные исследования или эксперименты были проведены для подтверждения данного вывода. Следовало предоставить данные о методах анализа, использованных для оценки корреляции между различными признаками, а также описать выборку и условия экспериментов. Наличие статистических данных, графиков или других визуальных материалов, иллюстрирующих уровень корреляции, существенно повысило бы убедительность представленных аргументов.

2. Предложенная автором мера близости демонстрирует значительное сходство с косинусным расстоянием, однако данное сходство не обсуждается в представленной

работе. Важно обратить внимание на необходимость анализа и четкого обоснования выбора данной метрики, особенно в контексте ее аналогии с косинусным расстоянием, которое широко используется в задачах обработки изображений и машинного обучения для оценки схожести векторов признаков. Следовало указать, каким образом авторская мера близости соотносится с косинусным расстоянием, а также рассмотреть преимущества и недостатки каждой из этих метрик в контексте решаемой задачи.

3. Не вполне ясна необходимость применения методов защиты биометрического шаблона от компрометации в контексте открытых биометрических образов лица, так как сам по себе образ лица не является секретной информацией. Полезно было бы провести детальный анализ целей и задач, для которых требуется внедрение таких защитных мер, включая оценку потенциальных рисков, связанных с использованием открытых биометрических данных. Например, рассмотреть возможность неправомерного использования или подделки биометрической информации с целью совершения мошеннических действий и уточнить, каким образом защита биометрического шаблона может минимизировать эти риски. Кроме того, следует обсудить концепцию конфиденциальности и безопасность личных данных в свете действующего законодательства, регулирующего обработку биометрической информации. Учитывая эти аспекты, целесообразно обосновать актуальность и необходимость мер защиты биометрического шаблона, даже если сами изображения лиц могут быть доступны публично, а также привести примеры сценариев, в которых применение технологий защиты может существенно повысить уровень безопасности аутентификации.

4. В представленной работе не обоснован выбор двух порогов в функции активации, что вызывает вопросы о целесообразности данного решения. Увеличение числа пороговых значений может потенциально улучшить показатели точности модели и повысить энтропию откликов при обработке входных данных нейросетевых преобразователей «биометрия-код» образов «Чужих». Это позволит более адекватно учитывать сложные зависимости в данных и повысить устойчивость модели к шумам. Поэтому было бы полезно исследовать возможность внедрения многопороговых функций активации для оптимизации работы нейросетевой модели.

5. Автор не указывает на дополнительные приложения, в которых нейросетевые преобразователи «биометрия-код» могут быть использованы для организации их «защищенного исполнения», помимо биометрической аутентификации. Важно рассмотреть широкий спектр потенциальных областей применения таких технологий, таких как системы мониторинга безопасности, автоматизация процессов идентификации в общественных местах и улучшение пользовательского опыта в различных сервисах, требующих высокой степени доверия. Также следует оценить возможность интеграции данных преобразователей в контексте многофакторной аутентификации и защиты конфиденциальной информации в рамках IoT-устройств. Указание на эти аспекты позволит лучше понять универсальность рассматриваемых технологий и их вклад в развитие безопасных систем обработки данных. Полезно было бы более подробно осветить данные вопросы для обоснования значимости исследования.

Необходимо отметить, что вышеуказанные замечания не влияют на общую положительную оценку научных результатов выполненного соискателем диссертационного исследования и не снижают ценности полученных результатов.

Заключение

Диссертационная работа Панфиловой Ирины Евгеньевны по своей новизне и практической значимости является законченной научно-квалификационной работой, решающей актуальную задачу повышения защищенности нейросетевой биометрической аутентификации по лицу.

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 Ирина Евгеньевна, заслуживает присуждения ученой степени кандидата технических наук по специальности 2.3.6. Методы и системы защиты информации, информационная безопасность.

Официальный оппонент:
Доктор физико-математических наук,
доцент, заведующий кафедрой
управления информационной
безопасностью, ФГБОУ ВО
«Уфимский университет науки и
технологий»

Исмагилова
Альбина Сабирьяновна

«20» 11 2024 г.

Докторская диссертация защищена по специальности 02.00.04 Физическая химия

Даю согласие на обработку персональных данных.

Адрес места основной работы:
450076, Республика Башкортостан, г. Уфа, ул. Заки Валиди, дом 32
Рабочий телефон: +7 (347) 273-66-92
Аадрес эл. почты: ismagilova.as@ugatu.su

Подпись Исмагиловой А.С.
Удостоверяю «20» 11 2024 г.
Начальник общего отдела УУНиТ
Рахимова Ж.Ф.