СИСТЕМЫ ЗАЩИТЫ БИОМЕТРИЧЕСКИХ ДАННЫХ

Азамжон Алиев
Студент Наманганского инженерно-строительного института

Мухтасар Заирджон кизи Мусаева
Студент Ургенчского филиала Ташкентского университета информационных технологий

АННОТАЦИЯ

В данной статье рассказывается о системах, обеспечивающих безопасность личных данных человека посредством его индивидуальных особенностей тела, таких как радужка, геометрия лица, руки, почерк и так далее.

Ключевые слова: защита, биометрия, человек, искусственный интеллект, личные данные, системы.

BIOMETRIC DATA PROTECTION SYSTEMS

Azamjon Aliyev
Student, Namangan Engineering Construction Institute

Mukhtasar Zayirjon qizi Musayeva
Student of Urgench branch of Tashkent University of Information Technologies

ABSTRACT

This article describes the systems that ensure the security of a person's personal data through their individual body features, such as the iris, face geometry, hands, handwriting, and so on.

Keywords: security, biometrics, human, artificial intelligence, personal data, systems.

ВВЕДЕНИЕ

В современном мире, где каждый пытается защитить свою частую и личную жизнь, большое внимание уделяется системам защиты. Люди ищут способы крепко и, главное, надежно закрыть данные от других. Будь то аккаунт в социальной сети или стратегически важный военный объект. В поисках

лучшей системы защиты широкое распространение получила биометрическая идентификация.

ЛИТЕРАТУРА И МЕТОДОЛОГИЯ

Представьте себе идеальную систему защиту, без традиционных замков и паролей, ключом к которой является сам человек. Она с фотографической точностью запоминает черты лица, внимательно вслушивается в скорость и тембр голоса, ощущает прикосновения и заглядывает прямо в глаза. Индивидуальность нельзя убрать или скопировать, значит, и получить доступ может лишь тот, кто внес свои данные. Так идеальна ли эта система? Что она из себя представляет?

Питание, воздух, характер, круг общения, перенесенные заболевания и даже домашние животные – все это делает каждого человека уникальным. На Земле нет двух совершенно одинаковых людей, ведь даже генетически симметричные близнецы не будут зеркальным отражением друг друга.

Как итог появилась эта система, основанная на биометрических данных человека. Существует шесть способов идентификации: аутентификация по сетчатке, по радужной оболочке глаз, геометрии руки и лица, голосовая и графическая защита. Давайте поговорим о каждой подробнее.

При сканировании сетчатки глаза используются инфракрасные лучи, которые запоминают и проверяют рисунок кровеносных сосудов внутри глаза. Однако из-за своей дороговизны и дискомфорта при проверке от этого метода практически отказались, перейдя к более простому и безопасному способу сканированию радужной оболочки глаза. Учеными доказано, что, в отличие от сетчатки, рисунок радужки не может изменяться с течением времени. Сложные врожденные компоненты рисунка позволяют фиксировать до двух сотен опорных точек, сканирование которых и устанавливает истинность объекта сканирования.

Геометрия руки и лица распространены куда больше, чем остальные виды идентификации. В современных смартфонах используется лишь отпечаток пальца, но в куда более сложных системах помимо самого отпечатка также учитываются и другие параметры. К примеру, толщина и длина пальцев, расстояние между суставами, длина фалангов, глубина ямки ладони. Чем больше параметров учитывается, тем надежнее будет защита.

РЕЗУЛЬТАТЫ И ОБСУЖДЕНИЕ

Во время сканирования лица система рассматривает расстояние между глазами, длину и форму губ, носа, разрез глаз, расположение бровей. Если у человека есть какие-то отличительные особенности вроде родинок или шрамов, то компьютер предусмотрит и это, сканируя. Упрощенный вариант этой системы защиты используется в телефонах, который просто сравнивает загруженное фото с человеком перед ним.

Голосовая и графическая идентификация относятся к динамическим системам защиты (т.е. к таким, биометрические данных человека которых могут изменяться с течением жизни). Голосовая аутентификация используется куда шире за счет своей простоты. Для построения шаблонов используют такие данные, как интонация, тембр, высота голоса, частота звука и т.д. Однако эта система имеет значительные недостатки. Например, голос человека меняется не только со временем, но и с состоянием здоровья, с настроением и тому подобным, что делает голосовую идентификацию довольно слабой.

Так же как и голосовая, графическая защита считается динамической системой. В ее параметры проверки входят данные о скорости и рефлективности рукописного ввода. Для этой системы используются специальные чувствительные поверхности. Помимо росписи как ключ могут быть использованы и какие-то фразы, и тогда система проверяет не только скорость, но и почерк, наклон букв, общие «штрихи» письма и особенности.
Биометрические системы довольно распространены, так как считаются на данный момент самыми надежными способами защиты информации. Упрощенные варианты используются в повседневной жизни в различных устройствах, начиная смартфонами и заканчивая умной техникой, к примеру, плитой или телевизором. Сложные комбинативные системы защиты используются в науке или на военных объектах, государственных образованиях. Политики используют биометрические данные как подпись. В Индии и некоторых странах Африки отпечатки пальцев или зубов так же являются своеобразной подписью.

Биометрические системы защиты распространены в массовой культуре. Например, в популярной игре «Among Us» для выполнения нескольких заданий необходимы биометрические данные персонажей. В мультфильме «Супер-семейка» дизайнер геройских костюмов использует биометрическую систему защиты для доступа к своему мини-ателье. Во многих фильмах в жанре научной фантастики такие системы также не стали исключением.

Но так ли идеальна эта система защиты? Есть ли возможность обойти ее? Примечательно то, что у самой теории дактилоскопических различий нет научных обоснований или доказательств. То есть, ученые так и не подтвердили то, что у каждого человека отпечатки полностью индивидуальны. Было множество случаев в криминалистике, когда по ошибке сажали не того лишь из-за того, что отпечатки совпадали на 98-99%, а для следователей это не так уж и мало.

Также отпечатки пальцев можно спокойно подделать. Если взять кусочек пластилина и приложить к нему палец нужного человека, сняв слепок, а потом залить полученную форму силиконом, то после застывания получится небольшой макет пальца с тем папиллярным рисунком, который необходим.
Пластические операции, грим, малейшие изменения в ракурсе – все это может повлиять на распознавание лица человека машиной. На Земле свыше 7 миллиардов людей, и есть вероятность, что внезапно найдется человек, который сможет пройти защиту, установленную под вас. Машина увидит то, что сможет распознать, а потому, если злоумышленнику удастся сделать свое лицо похожим на необходимое, он с легкостью проберется в любое устройство.

ЗАКЛЮЧЕНИЕ

Работа любой системы защиты имеет свои слабые места, которые возможно пробить. Каждая машина дает сбой или может совершить ошибку, хотя ученые и пытаются активно исправить это. С каждым годом появляются все новые и новые ступени развития искусственного интеллекта, машин учат распознавать людей по форме и длине ушей, по жестам и даже мимике.

Искусственные нейронные сети сканируют людей на улицах и в магазинах, могут распознать необходимый объект даже в полутьме или на большой скорости. Чем активнее развиваются технологии, чем активнее распространяется среди широких масс любовь к биометрическим системам защиты, тем опаснее становится жизнь человека и зависимее становится он сам. С каждым днем все больше людей добровольно проходят биометрическую идентификацию, тем самым подвергая себя опасности и риску окончательного безвольного подчинения.

REFERENCES

1. Сычев, Ю. Н. Защита информации и информационная безопасность: учебное пособие / Ю.Н. Сычев. – Москва : ИНФРА-М, 2021. – 201 с.