УДК 57.087
DOI 10.33764/2618-981X-2024-6-109-114

М. А. Козлов[1], А. Н. Поликанин[1]*

Оценка характеристик биометрической системы аутентификации

[1]Сибирский государственный университет геосистем и технологий, г. Новосибирск, Российская Федерация
*e-mail: lfmisok@gmail.com

Аннотация. В статье поднимается вопрос оценки характеристик разработанной авторами биометрической системы, соответствие системы действующим стандартам. Аутентификация в системе по биометрическим признакам понижает вероятность несанкционированного доступа к автоматизированному рабочему месту. Разработанная биометрическая система аутентификации основана на принципе распознавания изображения лица по контрольным точкам. Система автоматически определяет контрольные точки на лице, такие как расположения глаз, размеры губ, носа, щек. Для оценки характеристик применен метод статистического определения вероятностей. Результаты исследования показали, что стандартная камера, которая имеется практически на каждом автоматизированном рабочем месте, способна идентифицировать субъект. Также рассчитано расстояние, которого достаточно для идентификации лица человека. Экспериментальным путем было выяснено, что есть вероятность срабатывания системы не по эталону, а по фотографии субъекта. Для решения данной проблемы был добавлен второй фактор аутентификации в виде пароля, что в свою очередь в разы уменьшает вероятность несанкционированного доступа к автоматизированному рабочему месту.

Ключевые слова: биометрия, аутентификация, биометрические системы

M. A. Kozlov [1], A. N. Polikanin[1]*

Biometric systems used for access control in organizations

[1]Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation
*e-mail: lfmisok@gmail.com

Annotation. The article raises the issue of evaluating the characteristics of the biometric system developed by us, and the system's compliance with current standards. Authentication in the system based on biometric characteristics reduces the likelihood of unauthorized access to an automated workplace. The developed biometric authentication system is based on the principle of face image recognition by control points. The system automatically detects control points on the face, such as the location of the eyes, the size of the lips, nose, cheeks. The method of statistical determination of probabilities is used to evaluate the characteristics. The results of the study showed that a standard camera, which is available in almost every automated workplace, is able to identify the subject. The distance is also calculated, which is sufficient to identify a person's face. Experimentally, it was found out that there is a possibility that the system will work not according to the standard, but according to the photo of the subject. To solve this problem, a second authentication factor was added in the form of a password, which in turn significantly reduces the likelihood of unauthorized access to an automated workplace.

Keywords: biometrics, authentication, biometric systems

Введение

Создание программного продукта происходит поэтапно, начиная от идеи, определения характеристик, заканчивая тестированием и оценкой. Разработанный программный продукт, основанный на распознавании лиц, достиг этапа тестирования и оценки характеристик.

В рамках обзора литературы, отмечается, что существуют различные статистические методы, применяемые в различных сферах. В работе Бунимовича Е. А. и пособии Лаврусь О. Е. рассматриваются возможности применения статистических методов в науке и обиходе. Бунимович Е. А. акцентирует внимание на различие классического определения вероятности и статистического. Классическое связано с понятием благоприятствующего исхода, а статистической вероятностью события называется относительная частота появления этого события в произведенных испытаниях, что в свою очередь дает возможность применять метод в науке [2, 6].

В Российской Федерации существует несколько различных стандартов, которые регламентируют требования к различным системам:

– ГОСТ Р ИСО/МЭК 19795-1-2007 устанавливает общие требования к проведению эксплуатационных испытаний биометрических систем в отношении определения вероятности появления ошибок [1];

– ГОСТ Р ИСО/МЭК 19794-5-2013 определяет формат записи изображения лица в приложениях распознавания лица, условия и другие характеристики биометрических данных [5].

Ногин П. А. фокусируется на теоретических расчетах параметров оптической системы, с помощью которых можно рассчитать расстояния до изображения и их размеры [10].

Целью данного исследования является оценка разработанной биометрической системы, основанной на распознавании изображения лица.

Для достижения поставленной цели были решены следующие задачи:

– определить расстояние от камеры до объекта, которого достаточно для идентификации;

– сравнить показатели эксперимента с действующим ГОСТ Р ИСО/МЭК 19794-5-2013[5];

– оценить коэффициенты вероятности ложного недопуска (FRR).

Методы и материалы

Статистические методы широко используются в различных сферах для анализа и для вычисления и обобщения информации. Статистические методы — это научные методы описания и изучения различных явлений. Существует несколько различных видов статистических методов, например, метод статистического определения вероятности. Статистическое определение вероятности применяется, когда испытания могут быть воспроизведены неограниченное число раз при одном и том же комплексе условий. Вероятность рассчитывается по формуле [2]:

$$W_n(A) = \frac{m}{n}, \quad (1)$$

где $W(A)$ – вероятность; n – количество испытаний, в которых событие A появилось m раз.

Для начала исследования необходимо определить достаточно ли расстояние между камерой и объектом для работы системы. Расстояние определяется по формуле [9]:

$$D = \frac{f \cdot V}{v}, \quad (2)$$

где D – расстояние; f – фокусное расстояние; ν – размер изображения; V – реальные размеры объекта.

Для эксперимента использовалась видеокамера с определенными характеристиками, такими как фокусное расстояние, оптическое разрешение. Фокусное расстояние - физическая характеристика оптической системы, определяющая ее основные свойства [9]. Оптическое разрешение описывает объем реальной информации, который может передаваемый камерой [10]. В эксперименте использовалась камера Logitech c200 1,3 Мп, заявленное фокусное расстояние 3,6 мм [4]. Для корректного распознавания контрольных точек изображения лица необходимо иметь изображение лица, разрешение которого не менее 180 пикселей по горизонтали, а расстояние между центрами глаз не менее 90 пикселей [5]. Так как 1 см равен 37,938105 пикселям, конечные размеры изображения должны быть не менее 4,8 см по горизонтали, расстояние между центрами глаз не менее 2,38 см.

В случае добавления второго фактора, вероятность совместного появления двух независимых событий равна произведению их вероятностей, рассчитывается по формуле [2]:

$$P(AB) = P(A) \cdot P(B), \quad (3)$$

где P (AB) – вероятность; A, B – события; P(A) – вероятность события A; P(B) – вероятность события B; [6].

Для расчетов количества возможных комбинаций используется формула [7]:

$$a = I^n, \quad (4)$$

где a – количество комбинаций; n – количество позиций; I – количество символов, букв в одной позиции.

Результаты

Расстояние между камерой и объектом было выбрано 0,5 м, расстояние от подбородка до лба 0,19 м.

Исходя из расчетов, используя формулу 2, камера с фокусным расстоянием 3,60 мм, на расстоянии 0,5 м строит изображение размером 1,36 м. Соответственно данная камера удовлетворяет требованиям стандарта ИСО/МЭК 19794-5-2013 [5].

Протестировать систему согласилось 10

Эксперимент заключается в получении изображения лица субъекта, и обработке полученного изображение программой, пересчитывается расстояние между контрольными точками и сравнивает с имеющимися в базе значениями. Следующим этапом субъекта фотографируют на камеру мобильного телефона, и фотография предъявляется в объектив камеры системы биометрической аутентификации в качестве эталона, тем самым появляется понимание того, насколько система устойчива для различных попыток несанкционированного доступа, и требуются ли какие-нибудь доработки в части касающейся идентификации. Эксперимент проводился по 20 раз с участием человека и изображением человека на фотографии. Результаты эксперимента представлены в табл. 1.

Таблица 1

Результаты эксперимента

Номер субъекта	Количество попыток	Количество попыток аутентификации по фотографии	Количество раз допуска в систему натурального изображения	Количество раз недопуска в систему	Количество допуска фотографии	Количество недопуска фотографии
1	20	20	20	2	1	19
2	20	20	18	0	0	20
3	20	20	20	0	2	18
4	20	20	19	1	0	20
5	20	20	20	0	0	20
6	20	20	19	1	0	20
7	20	20	20	0	0	20
8	20	20	19	1	0	20
9	20	20	19	1	0	20
10	20	20	19	1	1	19

По полученным данным в табл. 1 производятся расчеты вероятностей, результаты расчетов представлены в табл. 2.

Таблица 2

Результаты расчетов вероятностей

P допуска	*P* недопуска	*P* допуска по фото	*P* недопуска по фото
0,965	0,035	0,020	0,980

Исходя из расчетов следует, система не может определить разницу между оригиналом и фотографией с вероятностью 0,02. Для решения этой проблемы введен второй фактор аутентификации, а именно пароль. Пароль - это условное слово или произвольный набор знаков, состоящий из букв, цифр и других символов, предназначенный для подтверждения личности или полномочий. Как правило пароль состоит из цифр и букв, есть вариант пин-кода, содержащего только цифры. Как правило пин-код используется в различных системах с низкой степенью безопасности, либо используется в качестве одного из факторов двухфакторной аутентификации [8].

Пароль, содержащий символы от 0 до 9. Количество вариантов комбинаций пароля a, состоящего из четырех символов, равна 10000 раз, вероятности угадать такой пароль P равна 0,0001, а также вероятность событий, при которых пароль будет угадан, а система распознает фотографию как настоящее лицо человека одновременно $P(AB)$ равна 0,000002.

Вероятность угадывания пароля, состоящего из 4 символов, рассчитанная по формуле (4), составляет 0,0001.

Соответственно вероятность событий, при которых пароль будет угадан, а система распознает фотографию как настоящее лицо человека, рассчитанная по формуле (3), 0,000002.

Заключение

Перед использованием фотографий субъектов, было получено согласие субъекта на обработку персональных данных в соответствии с ФЗ-152 «О персональных данных» [3]. Таким образом, в настоящей работе проведены расчеты расстояния детекции в соответствии с государственным стандартом, проведен эксперимент по определению вероятности ложного недопуска (FRR) и вероятность допуска по фотографии вместо эталона, вследствие чего система доработана вторым фактором аутентификации. В совокупности оба фактора аутентификации снижают возможность несанкционированного доступа до вероятности 0,000002.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. ГОСТ Р ИСО/МЭК 19795-1-2007. Автоматическая идентификация. Идентификация биометрическая : национальный стандарт Российской Федерации : издание официальное : утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 25 декабря 2008 г. N 403-ст : введен впервые : дата введения 2009-01-01 / разработан научно-исследовательским институтом биометрической техники Московского государственного технического университета имени Н.Э.Баумана (НИИ БМТ МГТУ им.Н.Э.Баумана) — М. : Стандартинформ, 2019 — 48 с.

2. Лаврусь О. Е. Конспект лекций по теории вероятностей / О. Е. Лаврусь. – Самарская государственная академия путей сообщения. — Самара : СГАПС, 2007. — 135 с.

3. Российская Федерация. Законы. О персональных данных : Федеральный закон №152-ФЗ : принят Государственной думой 27 июля 2006 года : одобрен Советом Федерации 14 июля 2006 года].

4. Logitech : официальный сайт. – Лозана. обновляется в течение суток – URL: https://support.logi.com/hc/en-au/articles/360023462133-C210-Technical-Specifications

5. ГОСТ Р ИСО/МЭК 19794-5-2013. Биометрия. Форматы обмена биометрическими данными. Часть 5. Данные изображения лица : национальный стандарт Российской Федерации : издание официальное : утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 6 сентября 2013 г. N 987-ст : введен взамен ГОСТ Р ИСО/МЭК 19794-5-2006 : дата введения 2015-01-01 / разработан научно-исследовательским институтом биометрической техники Московского государственного технического университета имени Н.Э.Баумана (НИИ БМТ МГТУ им. Н.Э.Баумана) – М.: Стандартинформ 2019 — 109 с.

6. Бунимович Е. А. Вероятность и статистика / Е. А. Бунимович. — М. :Просвещение. — 2024. — 144 с.

7. Трушин Б. В. Комбинаторика / Б. В. Трушин // М.: Эксмо. — 2023. — 240 с.

8. Сысоев А. Пароль / А. Сысоев // Ridero. — Екатеринбург 2023. — 105с.

9. Михеенко А. В. Геометрическая оптика / А. В. Михеенко // Тихоокеанский государственный университет. — Хабаровск : ТОГУ, 2018. — 104 с.

10. Ногин П. А. Фотоаппараты и оптика / П. А. Ногин // М.: Искусство. — 1958. — 144 с.

11. Базанов П.В. Биометрическая система идентификации человека по изображениям лица / П. В. Базанов // Вестник Московского университета – 2006. – № 1. – С. 49–55.