УДК 004.93
DOI 10.33764/2618-981X-2023-6-160-164

Е. К. Малютин[1], Г. В. Попков[1,2]*

Анализ эффективности программ распознавания образов

[1] Сибирский государственный университет геосистем и технологий, г. Новосибирск, Российская Федерация
[2] Сибирский государственный университет телекоммуникаций и информатики, г. Новосибирск, Российская Федерация
* e-mail: shuklinaa@list.ru

Аннотация. В статье проведен анализ некоторых программ, соответствующих тематике статьи. Выбранные программы были исследованы. Их функции и специализация была проверена экспериментальным путем, позволяя изучить эффективность их технических характеристик для сравнения и анализа. Также были проведены мероприятия по объединению целей их изначальных алгоритмов. В связи с различной темой выбранных для экспериментального анализа программ к ним применялся разный подход. Дополнительно были выявлены их сильные и слабые стороны, позволяя на основе этих данных построить новую тропу, ведущую хоть и не по-новому, но относительно свободному пути, который на основе объединения и взаимного дополнения позволит упростить взаимодействие и расширить возможности как для собственника информации, так и для владельца программы.

Ключевые слова: распознавания образов, IOS, Android, программа, сравнение эффективности

E. K. Malyutin[1], G. V. Popkov[1,2]*

Analysis of the effectiveness of image recognition programs

[1] Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation
[2] Siberian State University of Telecommunications and Informatics, Novosibirsk, Russian Federation
* e-mail: shuklinaa@list.ru

Abstract. The article analyzes some programs, corresponding to the subject of the article. Selected programs were researched. Their functions and specializations have been experimentally tested, allowing the effectiveness of their technical characteristics to be studied for comparison and analysis. Activities were also carried out to combine the goals of their original algorithms. Due to the different topics chosen for the experimental analysis of the programs, a different approach was applied to them. Additionally, their strengths and weaknesses were identified, allowing, on the basis of these data, to build a new path leading, although not in a new way, but in a relatively free way, which, based on association and mutual complementation, will simplify interaction and expand opportunities, both for the owner of information, and for the owner of the program.

Keywords: image recognition, IOS, Android, program, efficiency comparison

Введение

Для защиты личной информации человек придумывал, придумывает и будет придумывать все более совершенные методы, в том числе в области защиты информации.

В настоящее время защита персонифицированной информации имеет тенденцию роста, так как в современных реалиях злоумышленники становятся изощреннее в обманных методах сбора информации, что представляет опасность как для общества, так и для отдельного индивида.

Самые уязвимые места – это мобильные устройства, доступ к которым, можно получить самым прямым и быстрым способом, а обладая им, легко управлять всеми сферами жизни современного человека. Это вынуждает каждого иметь действенный способ защиты информации. Однако каждый способ основан на распознавании образов, что выражается как в числовом коде, так и в биометрических данных [1].

Анализ публикаций на эту тему показывает, что их количество невелико, а из опубликованных большинство являются описанием преимуществ или метода работы программы.

В связи с этим целью статьи является сравнительный анализ возможностей и технической обеспеченности программ на базе IOS и Android для дополнительной защиты персонифицированной информации.

Анализ проведен по следующим критериям: вариативность, скорость обработки и эффективность.

Методы и материалы

Программы, основанные на образах, создаются и улучшаются для постоянного увеличения уровня защищенности. Основными методами защиты информации в этих программах являются: числовой пароль, отпечаток пальца и биометрический снимок лица.

В настоящее время многие пользователи персональных устройств, заинтересованные в безопасности личной информации, используют для защиты отпечаток пальца или лица. Операционные системы (ОС) персональных устройств предоставляют базовый уровень подобной защиты, однако, защитить персонифицированную информацию они не в силах. Для создания многоуровневой защиты используются дополнительные программы, обеспечивающие более высокий уровень защищенности и возможность выборочной защиты информации. Для оценки любой биометрической системы используют два параметра:

– FAR (False Acceptance Rate) – коэффициент ложного пропуска, т.е. процент возникновения ситуаций, когда система разрешает доступ пользователю, незарегистрированному в системе;

– FRR (False Rejection Rate) – коэффициент ложного отказа, т.е. отказ в доступе зарегистрированному пользователю системы [2, 3].

Данные параметры получают расчетным путем, в основе которого лежит метод математической статистики. Чем ниже значение, тем выше точность распознавания. Средние значения FAR и FRR представлены в табл. 1.

Эти данные не являются абсолютными, однако позволяют выбрать в настоящее время наиболее эффективный метод защиты информации для персональных устройств из доступных методов. На главных ОС современности программы дополнительной защиты распознают лица своих владельцев в режиме реального

времени минимум по 80 узловым точкам. Примером являются программы: «IObit Applock» с платформы Android и «BioID» на базе IOS [4, 5].

Таблица 1

Средние значения FAR и FRR для распространенных способов биометрической идентификации

Способ биометрической идентификации	FAR, %	FRR, %
Отпечаток пальца	0,001	0,6
Распознавание лица 2D	0,1	2,5
Распознавание лица 3D	0,0005	0,1

«IObit Applock» является уникальной программой для дополнительной защиты персонифицированных данных по желанию пользователя.

Особенность этой программы заключается в возможности создания индивидуального ключа-образа на основе воображения (рис. 1) [4]. Уровень защиты информации при данном методе признан наивысшим, так как возможность кражи такого ключа исключена. Однако его сложность так же является высокой, так как созданный таким методом ключ уникален и должен быть повторен в точности.

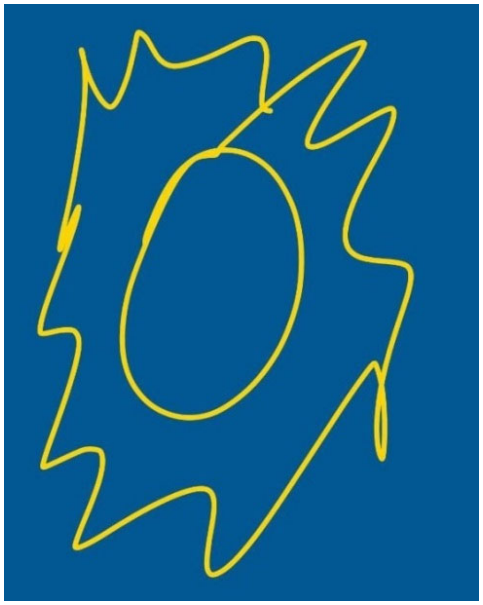

Рис. 1. Пример индивидуального ключа-образа

«BioID» является инновационным продуктом интеллектуального творчества, способным к распознаванию глаз для частично прикрытых лиц (рис. 2) [5]. Такой алгоритм распознавания позволяет увеличить уровень защищенности, при уменьшении объема обрабатываемой информации, что соответствует современным реалиям, позволяя получить доступ к защищенной информации в общественных местах быстро и безопасно.

Рис. 2. Пример периокулярного распознавания

Результаты

В результате выполненных исследований на основе изучения тематической информации из технической литературы был проведен сравнительный анализ по следующим критериям: вариативность, скорость обработки и эффективность.

Сравнение проводилось на основе заявленных разработчиком данных, а также экспериментально рассчитанных в лабораторных условиях значения. Преимущества программы в критериях будет показано знаком «+», если она уступает – знаком «–», преимущества их квалификации минимизирует ущерб от недостатков – знаком «+/–». Результаты представлены в табл. 2.

Таблица 2

Преимущества характеристик программ защиты персональных данных

Критерии	IObit Applock	BioID
Вариативность	+	-
Скорость обработки	-	+/-
Эффективность	+/-	+/-

В ходе проведенной работы было выявлено, что программа IObit Applock имеет весь спектр способов защиты информации, возможных для персональных устройств, а именно: PIN-код, отпечаток пальца, биометрию лица и графический пароль, который так же представлен в виде произвольного рисунка. Тогда как BioID специализируется на биометрическом снимке лица, однако его уровень осведомленности позволяет проводить аутентификацию по ограниченной площади лица, что способствует более высокой степени защиты информации и минимизации FRR [6, 7].

В лабораторных экспериментах проведены подсчеты скорости обработки образа для получения доступа пользователя к информации. Эксперимент показал, что программе IObit Applock требуется не более 1,5 секунд на обработку поступающего образа для аутентификации, однако, в случае произвольного графического пароля временной диапазон увеличивается пропорционально сложности и точности воспроизведения последнего, что приводит к высокой степени защиты персональных данных. Временные показатели программы BioID имеют диапазон от 1 секунды (при полном доступе к биометрии лица, без внешнего вмешательства) до 5 секунд (при частичном сокрытии и плохой освещенности) [8].

Критерий эффективности был исследован по уровню сложности системы защиты. Проанализировав IObit Applock и BioID, можно утверждать, что первый имеет самый высокий уровень безопасности, так как произвольный графический пароль повторить или взломать невозможно. Однако, остальные способы аутентификации IObit Applock равны, а в случае с биометрией лица BioID уступают, из-за чего критерий эффективности для каждой программы равнозначен, так как у каждой есть преимущественная черта, на которой она специализируется.

Заключение

Сравнительный анализ характеристик рассмотренных программ позволяет сделать вывод о том, что преимущество в области спецификации и метод, на который делает акцент данная программа, обладают большей самостоятельной эффективностью в защите персональных данных. Так же следует отметить, что метод периокулярного распознавания программы BioID является очень эффективным для защиты как персональных данных, так и самого мобильного устройства. Однако проблема угрозы конфиденциальной информации остается не решенной окончательно, так как кражи личных данных продолжаются и в настоящее время не только не намечается спад, а заметен рост краж с последующей публикацией в общественном доступе или с целью шантажа. Одним из возможных путей решения данной проблемы является синтез преимуществ программ распознавания образов, используемых для защиты персональных данных, подобные тем, что рассмотрены выше. Таким образом, в дальнейшем исследовании полученные данные и результаты сравнительного анализа, будут использованы для синтеза новой программы, которая, объединив преимущества других, сможет решать более широкий спектр задач при высокой скорости и большей эффективности [9, 10].

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Царев А.Г. Принципы и методы автоматического распознавания образов // Труды Международного симпозиума «Надежность и качество» – Пенза, 2010. – Т.1. – С. 56 – 58.

2. Растригин Л. А., Эренштейн Р. Х. Метод коллективного распознавания: учебник. Москва: Энергоиздат, 2006. 80 с.

3. Потапов А.С. Распознавание образов и машинное восприятие: учебник. Санкт-Петербург: Политехника, 2019. – 548 с.

4. Разработчик программы IObit Applock. URL: http://www.spsoftmobile.com/ (дата обращения: 28.03.2023).

5. Разработчик программы BioID. URL: http://www.bioid.com/ (дата обращения: 28.03.2023).

6. Фу К. Структурные методы в распознавании образов: учебник. Москва: Мир, 2005. – 144 с.

7. Мазуров В.Д. Комитеты систем неравенств и задача распознавания // Кибернетика – Москва, 2004. – № 2. – С. 140-146.

8. Айзерман М.А., Браверман Э.М., Розоноэр Л.И. Метод потенциальных функций в теории обучения маши: учебное пособие. Москва: Наука, 2018. – 264 с.

9. Журавлев Ю.И. Об алгебраическом подходе к решению задач распознавания или классификации // Проблемы кибернетики – Москва, 2015. – № 33. – С. 5-68.

10. Горбань А., Россиев Д. Нейронные сети на персональном компьютере: учебник. Новосибирск: Наука, 2016. – 278 с.