www.volsu.ru

DOI: https://doi.org/10.15688/NBIT.jvolsu.2020.1.3

УДК 004.93
ББК 32.813.52

ПОДХОДЫ К ЗАЩИТЕ СИСТЕМ ВИДЕОНАБЛЮДЕНИЯ ПРИ ПРИМЕНЕНИИ АЛГОРИТМОВ РАСПОЗНАВАНИЯ

Татьяна Александровна Попова

Ассистент кафедры информационной безопасности,
Волгоградский государственный университет
infsec@volsu.ru
просп. Университетский, 100, 400062 г. Волгоград, Российская Федерация

Анатолий Михайлович Афанасьев

Доктор технических наук, профессор кафедры информационной безопасности,
Волгоградский государственный университет
infsec@volsu.ru
просп. Университетский, 100, 400062 г. Волгоград, Российская Федерация

Григорий Владимирович Жарков

Студент кафедры информационной безопасности,
Волгоградский государственный университет
g89954113431@yandex.ru
просп. Университетский, 100, 400062 г. Волгоград, Российская Федерация

Аннотация. Определены уязвимости алгоритмов распознавания объектов и лиц. Выявлены подходы к защите систем видеонаблюдения при применении алгоритмов распознавания. Проведен анализ эффективности мер защиты.

Ключевые слова: информационная безопасность, распознавание объектов, распознавание лиц, уязвимости алгоритмов распознавания, меры защиты.

Системы с алгоритмами распознавания – новый шаг в развитии методов аутентификации, в настоящее время такие алгоритмы применяются повсеместно [1; 2]. В операционных системах уже есть технологии распознавания лиц, так как это позволяет входить в систему в три раза быстрее, чем при входе с паролем и практически каждый смартфон в наше время поддерживает функцию разблокировки с помощью камеры. Распознавание объектов, в свою очередь, может применяться при аутентификации автомобилей, при въезде на контролируемую территорию и зачастую играет немаловажную роль в реализации безопасности предприятий [3].

При явных преимуществах, системы распознавания с некоторой вероятностью могут выдавать ложный результат. Важными характеристиками любой биометрической системы являются ошибки первого и второго рода (см. рисунок).

FAR (False Acceptence Rate) – вероятность, что неавторизованный пользователь/

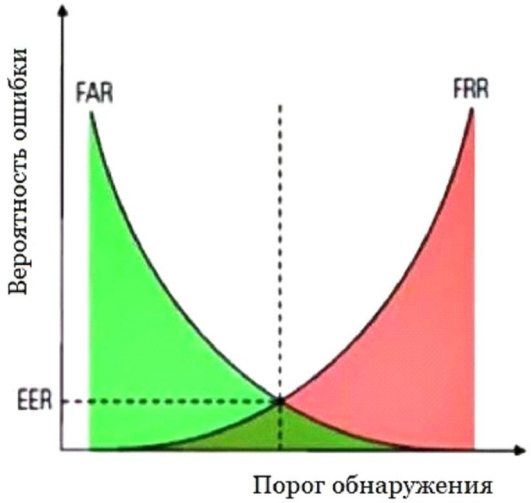

График зависимости вероятности ошибки от порога обнаружения

объект будет распознан как авторизованный (ошибка 1-го рода).

FRR (False Rejection Rate) – вероятность, что авторизованный пользователь/объект будет неправильно распознан (ошибка 2-го рода).

EER (Equal Error Rate) – точка равновесия, в которой FAR и ERR пересекаются.

Ошибки 2-го рода не несут ущерба при применении алгоритмов распознавания для аутентификации, в то время как ошибки 1-го рода являются опасными, так как позволяют злоумышленнику получить доступ к конфиденциальной информации. Таким образом, уязвимостями алгоритмов распознавания будем считать методы достижения ошибок 1-го рода.

На сегодняшний день существует несколько уязвимостей алгоритмов распознавания:

1) Фото цели (V1). Это может быть как распечатанная фотография так и изображение с какого-нибудь устройства, например телефона или планшета. Подавляющее большинство простых методов распознавания до сих пор можно обмануть этим способом. Злоумышленник может сфотографировать цель или найти фотографию в интернете, например в социальных сетях.

2) Видеозапись цели (V2). Видеозапись можно использовать и для взлома более сложных алгоритмов распознавания, где проверяется подлинность цели путем анализа нескольких ракурсов.

3) 3D макет (V3). Более сложный и затратный вариант, заключает в себе создание трехмерной модели объекта. В случае с распознаванием лица – объектом выступает 3D модель головы. Очевидно, что получить слепок лица жертвы является довольно сложной задачей в реальной жизни, поэтому злоумышленники используют глубокие нейронные сети, которые прогнозируют 3D форму лица по набору фотографий или по видео. После этого злоумышленник может распечатать на 3D принтере скульптуру лица или сделать маску.

4) Специальный макияж, грим (V4). Используя профессиональный грим, злоумышленник может загримировать себя под сотрудника.

5) Случайное ложное срабатывание (V5). В случае малого количества отличительных черт объекта распознавания, его легко можно спутать с похожими на него другими объектами.

6) Взлом алгоритмов распознавания (V6). Сложная в реализации уязвимость, которая предполагает использование внутренних уязвимостей самого алгоритма распознавания.

Увеличить защищенность алгоритмов распознавания можно применив следующие меры защиты:

1) Анализ нескольких ракурсов изображения объекта. Анализируется не один кадр, а временной ряд и по временному ряду оценивается подлинность объекта. Недостатком такого метода является необходимость в дополнительном времени на проверку.

2) Совершение определенных действий пользователем. Похож на предыдущий пункт, только анализируется не любое изменение

ракурса, а соответствие поведения человека требуемым действиям.

3) Проверка фона. Данная мера защиты актуальна при расположении камеры в определенном месте. Если камера детектирует, что фон отличается от обычного, то это может значить, что используется фотография или видео объекта.

4) Искажение при движении. Если злоумышленник использует устройство с изображением объекта, при движении устройства могут возникать блики или неестественное размытие, это можно задетектировать. Также можно обнаружить использование злоумышленником распечатанной фотографии, за счет того, что в каждой камере есть линза и при движении объекта меняется фокусное расстояние, в линзе изображение искажается, и, проведя анализ этих искажений, можно понять, что перед камерой плоское изображение.

5) Распределение освещения. Распределение освещения на объекте и на окружении объекта позволит узнать настоящий ли объект перед камерой.

6) Добавление отличительных черт объекту. Оригинальная цветная наклейка увеличит оригинальность объекту распознавания.

7) Использование специальных камер (ИК-камер, 3D-камер). Заключается в использовании специального оборудования. Лучший результат дает комбинирование нескольких типов таких камер. Такие камеры не требуют никакого кооператива со стороны пользователей, но их использование требует больших затрат.

8) Дополнительные способы идентификации. Проверяются дополнительные характеристики объекта, например отпечатки пальцев.

В таблице представлен сравнительный анализ эффективности мер защиты. По результатам анализа, было определено, что дополнительные способы идентификации перекрывают все уязвимости алгоритма распознавания лиц, но этот способ очень затратный. Другой эффективной мерой защиты является совершение определенных действий пользователем, эта мера перекрывает три из шести уязвимостей и является простой в реализации и низкой по стоимости.

Для алгоритмов распознавания объектов, такие меры защиты как добавление отличительных черт объекту и проверка фона или распределение освещения, являются самыми оптимальными и перекрывают три из пяти уязвимостей.

СПИСОК ЛИТЕРАТУРЫ

1. ГОСТ Р 50.1.053-2005. Информационные технологии. Основные термины и определения в области технической защиты информации : дата введения 2006-01-01. – М. : Стандартинформ, 2005.

Сравнительный анализ эффективности мер защиты

Методы защиты	Перекрываемые уязвимости	Алгоритмы	Простота реализации	Стоимость
Анализ нескольких ракурсов изображения объекта	V1	Распознавания лиц и объектов	Низкая	Низкая
Совершение определенных действий пользователем	V1, V2, V3	Распознавания лиц	Низкая	Низкая
Проверка фона	V1, V2	Распознавания лиц и объектов	Средняя	Низкая
Искажение при движении	V1, V2	Распознавания лиц и объектов	Высокая	Низкая
Распределение освещения	V1, V2	Распознавания лиц и объектов	Средняя	Низкая
Добавление отличительных черт объекту	V5	Распознавания объектов	Низкая	Низкая
Использование специальных камер (ИК, 3D).	V1, V2	Распознавания лиц и объектов	Низкая	Высокая
Дополнительные способы идентификации	V1, V2, V3, V4 (частично), V5, V6	Распознавания лиц	Низкая	Высокая

2. ГОСТ Р 51558-2008. Средства и системы охранные телевизионные. Классификация. Общие технические требования. Методы испытаний : дата введения 2009-09-01. – М. : Стандартинформ, 2009.

3. Попов, Г. А. Разработка программного комплекса видеоконтроля объектов или лиц на территории организации / Г. А. Попов, Т. А. Попова // Актуальные вопросы информационной безопасности регионов в условиях перехода России к цифровой экономике : материалы VII Всероссийской научно-практической конференции, г. Волгоград, 26–27 апр. 2018 г. – Волгоград : Изд-во ВолГУ, 2018. – С. 285–289.

REFERENCES

1. *GOST R 50.1.053-2005. Informatsyonnye tekhnologii. Osnovnye terminy i opredeleniya v oblasti tehnicheskoj zashchity informatsii: data vvedeniya 2006-01-01* [Information Technology. Basic Terms and Definitions in the Field of Technical Information Security. Date of Introduction 2006-01-01]. Moscow, Standartinform, 2005.

2. *GOST R 51558-2008. Sredstva i sistemy okhrannye televizionnye. Klassifikatsyya. Obshchie tekhnicheskie trebovaniya. Metody ispytanij: data vvedeniya 2009-09-01* [TV security Equipment and Systems. Classification. General Technical Requirements. Test method. Date of Introduction 2009-09-01]. Moscow, Standartinform, 2009.

3. Popov G.A., Popova T.A. Razrabotka programmnogo kompleksa videokontrolya obyektov ili lits na territorii organizatsii [Development of a Software Package for Video Monitoring of Objects or Persons on the Territory of the Organization]. *Aktualnye voprosy informatsionnoy bezopasnosti regionov v usloviyakh perekhoda Rossii k tsifrovoy ekonomike: materialy VII Vserossiyskoy nauchno-prakticheskoy konferentsii, g. Volgograd, 26–27 apr. 2018 g.* [Topical Issues of Regional Information Security in the Context of Russia's Transition to the Digital Economy. proceedings of the 7th All-Russian Scientific and Practical Conference, Volgograd, April 26–27, 2018]. Volgograd, Izd-vo VolGU, 2018, pp. 285-289.

APPROACHES TO THE PROTECTION OF VIDEO SURVEILLANCE SYSTEMS WHEN APPLYING RECOGNITION ALGORITHMS

Tatiana A. Popova

Assistant Lecturer, Department of Information Security,
Volgograd State University
infsec@volsu.ru
Prosp. Universitetsky, 100, 400062 Volgograd, Russian Federation

Anatoly M. Afanasiev

Doctor of Sciences (Engineering), Professor, Information Security Department,
Volgograd State University
infsec@volsu.ru
Prosp. Universitetsky, 100, 400062 Volgograd, Russian Federation

Grigorij V. Zharkov

Student, Department of Information Security,
Volgograd State University
g89954113431@yandex.ru
Prosp. Universitetsky, 100, 400062 Volgograd, Russian Federation

Abstract. A system with detection algorithms is a new step in the development of authentication methods. Currently these algorithms are used everywhere. Operating systems already have the facial recognition technology, as it allows a person to log in three times faster than when logging in with a password, and almost every smartphone today supports the function of unlocking with a

camera. Object recognition, in turn, can be used for vehicle authentication, when entering a controlled territory, and often plays an important role in implementing enterprise security.

With obvious advantages, recognition systems are more likely to produce false results. Important characteristics of any biometric system are errors of the first and second kind.

The paper identifies vulnerabilities in object and face recognition algorithms. Approaches to the protection of video surveillance systems when using recognition algorithms are defined. The analysis of the effectiveness of protective measures is carried out.

Based on the results of the analysis, it has been determined that additional identification methods cover all the vulnerabilities of the facial recognition algorithm, but this method is very expensive. Another effective measure of protection is the performance of specific actions by the user. This measure covers three of the six vulnerabilities, and is easy to implement and has a low cost.

Key words: information security, object recognition, face recognition, recognition algorithm vulnerabilities, protection measures.