УДК 004.932

ДЕТЕКТОР САБОТАЖА ДЛЯ ВСТРАИВАЕМОГО В СИСТЕМЫ ВИДЕОНАБЛЮДЕНИЯ МОДУЛЯ ОБНАРУЖЕНИЯ ДЫМА

Е. Р. Адамовский, Н. А. Томашевич, Р. П. Богуш

Полоцкий государственный университет имени Евфросинии Полоцкой, Полоцк, Республика Беларусь, e.adamovsky@psu.by

В статье рассматривается задача автоматического обнаружения саботажа для систем видеонаблюдения. Представлена архитектура модуля обнаружения дыма с функциями определения перекрытия объектива сторонними предметами. Описан алгоритм выявления саботажа. Разработанные решения реализованы в программно-аппаратном комплексе на базе одноплатного компьютера, при этом предусмотрена его интеграция в систему видеонаблюдения. Выполнены экспериментальные исследования и представлены результаты, подтверждающие перспективность практического применения разработанного решения.

Ключевые слова: обнаружение дыма; компьютерное зрение; выявление аномалий; резкость изображений.

SABOTAGE DETECTOR FOR EMBEDDED SMOKE DETECTION MODULE IN SURVEILLANCE SYSTEMS

Y. R. Adamovskiy, N. A. Tomashevich, R. P. Bohush

Euphrosyne Polotskaya State University of Polotsk, Polotsk, Belarus, e.adamovsky@psu.by

The paper discusses the problem of automatic detection of sabotage for video surveillance systems. The architecture of the smoke detection module with functions of determining the lens overlap with foreign objects is presented. The algorithm for detecting sabotage is described. The developed solutions are implemented in a software and hardware complex based on a single-board computer, while its integration into the video surveillance system is provided. Experimental studies are carried out. The results of experiments confirming the prospects of practical application are presented.

Keywords: smoke detection; computer vision; anomaly detection; image sharpening.

1. Введение

Развитие методов компьютерного зрения позволяет расширять набор прикладных задач, решаемых с применением систем видеонаблюдения. Видеодетекторы раннего обнаружения пожара являются перспективными

для использования как в помещениях разных размеров, включая большие протяженные, так и на открытых пространствах [1, 2]. Внедрение их в существующие системы видеонаблюдения позволит значительно повысить эффективность раннего мониторинга пожаров. Однако при этом возрастает необходимость быстрого выявления аномалий, приводящих к отсутствию видеосигнала, среди которых выделяется преднамеренный саботаж, представляющий собой действие, направленное на срыв работы подвергающейся атаке системы видеонаблюдения. Отличие от вандализма заключается в стремлении злоумышленников в течение определенного времени сохранять видимость ее нормального функционирования. Такая особенность является критической для раннего обнаружения пожара. При саботаже может осуществляться физическое воздействие на камеры видеонаблюдения путем перекрытия их объективов непрозрачными или полупрозрачными объектами, или закрашиванием, в результате чего фиксация действий злоумышленников или детектирование визуальных признаков пожара окажется невозможной. Сотруднику службы безопасности затруднительно постоянно и единовременно отслеживать корректность работы большого количества камер. Как следствие, может быть нанесен значительный материальный ущерб в случае пропуска возгорания на ранней стадии. Алгоритмы автоматического обнаружения саботажа должны учитывать сложные условия, возникающих в реальных условиях работы [3]. В том числе не должно быть большого количества ложных срабатываний, которые связаны с непреднамеренными действиями людей или природными явлениями. Например, перекрытие объектива может происходить, когда перед камерой проходит толпа людей или крупный объект, что может привести к ложному срабатыванию. Кратковременные колебания камеры из-за порывов ветра хотя и не приводят к постоянному изменению поля обзора, но также могут вызывать ложные срабатывания детекторов саботажа. Резкое изменение уровня освещенности, выключение света в помещении, может привести к ошибочной тревоге. Поэтому в настоящее время существует ряд подходов для обнаружения преднамеренного саботажа. Система признаков формируется с помощью фильтров, которые анализируются во времени, при этом для подавления ложных тревог используется фильтр Калмана в [4]. Анализ четкости границ объектов в кадрах на определенном временном интервале используется в работе [5]. В [6] предложено использовать алгоритмы глубокого обучения для выявления и категоризации частых случаев несанкционированного доступа: расфокусировка, затенение и изменение ориентации видеокамеры. Однако такой подход вычислительно сложен для автономного модуля, в котором выполняется также и обнаружение дыма. Таким образом, разработка и использова-

ние эффективного автоматического детектора саботажа с хорошими качественными характеристиками, но не требующего больших вычислительных затрат, для встраиваемых модулей систем видеонаблюдения является актуальной задачей.

2. Общая архитектура модуля обнаружения дыма с функцией детектирования саботажа

Архитектура разработанного модуля показана на рис. 1 и включает: IP-камеру, которая генерирует исходный видеопоток; веб-приложение для управления комплексом; одноплатный компьютерRaspberry Pi 4B, выполняющий прием видеопотока, детектирование дыма и саботажа, формирование выходного видеопотока; коммутатор, соединяющий все узлы комплекса; средство просмотра выходного видеопотока.

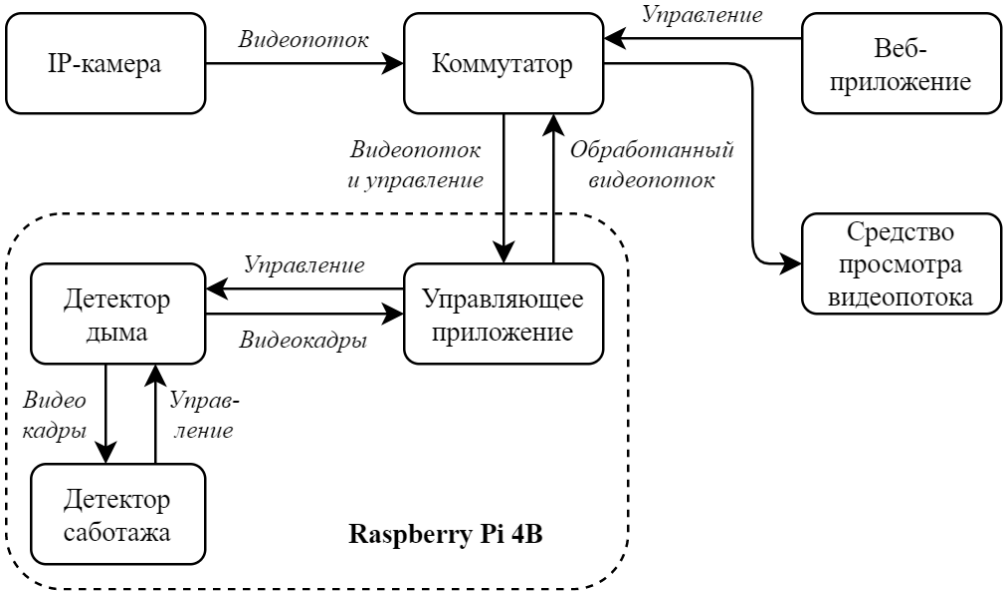

Рис. 1. Общая архитектура встраиваемого модуля обнаружения дыма с детектором саботажа

Программное обеспечение Raspberry Pi 4B включает управляющее приложение Server, которое выполняет кодирование и декодирование видеопотоков, а также управляет модулем детектора дыма FireApp, который включает в себя модуль детектора саботажа, передает видеокадры и по его команде меняет режим работы.

Алгоритм детектирования дыма [7] реализован на C++ использованием функций библиотеки машинного зрения OpenCV 4.7.0 и выступает в качестве основы приложения FireApp. Начальным состоянием является

режим запуска, при этом основные этапы алгоритма, а также модуль детектирования саботажа не инициализируются в течение заданного времени, пока выполняется построение модели фона анализируемой сцены. Далее алгоритм переходит в основной режим работы, который включает модули обнаружения дыма и саботажа.

3. Алгоритм обработки видеопоследовательности для детектирования саботажа

К основным действиям злоумышленников для систем видеонаблюдения со стационарными видеокамерами относятся: перекрытие объектива непрозрачным объектом светлого или темного цвета, либо перекрытие полупрозрачным объектом для расфокусировки изображения в кадре.

С учетом обеспечения максимизации эффективности работы при минимизации временных затрат, для обеспечения реального режима обработки видео на одноплатном компьютере используется особенность оптической системы камер видеонаблюдения, для которой минимальная дистанция фокусировки которых составляет десятки сантиметров. Тогда, при перекрытии камеры близким объектом, резкость изображения будет снижена. Данный алгоритм предполагает следующие основные шаги.

1. Цветное изображение *RGB* конвертируется в черно-белое *GRAY* путем объединения его цветовых каналов.

$$GRAY = 0.299R + 0.587G + 0.114B. \tag{1}$$

2. Вычисляется Лапласиан L полученного изображения, который показывает, насколько значение пикселя отличается от среднего значения его окрестности, как результат свертки с маской:

$$L = \begin{bmatrix} 0 & 1 & 0 \\ 1 & -4 & 1 \\ 0 & 1 & 0 \end{bmatrix} * GRAY. \tag{2}$$

3. Для L при векторном представлении изображения вычисляется стандартное отклонение как:

$$\sigma = \sqrt{\frac{\sum\left(x_i - \bar{x}\right)^2}{N}}, \tag{3}$$

где x_i – значение пикселя полутонового изображения; $\bar{x}$ – среднее значение для всех пикселей; N – общее количество пикселей в изображении.

4. Полученное значение σ используется в качестве параметра, который оценивает резкость изображения.

5. Принимается решение о саботаже, если выполняется условие:

$$\sigma < \sigma_{th}, \tag{4}$$

где σ_{th} – пороговое значение.

4. Результаты экспериментов

С целью проверки корректности работы детектора саботажа был подготовлен набор изображений, разделенный на три класса по их содержимому: исходные кадры видеопоследовательности, изображения с видеокамеры после перекрытия объектива светлым объектом, изображения с видеокамеры после перекрытия объектива темным объектом. Примеры изображений показаны на рис. 2.

Для данного набора изображений применялся алгоритм выявления саботажа, и оценивалась корректность его работы. Результаты оценки резкости изображений: от 13,95 до 22,01 для кадров обычной сцены; от 1,83 до 2,89 для кадров, полученных после перекрытия объектива объектом светлого цвета; от 4,77 до 8,36 для изображений, полученных после перекрытия объектива объектом темного цвета. Таким образом, установлено, что при пороговом значении σ_{th} = 10 все изображения могут быть классифицированы корректно. Время обработки одного кадра разрешения 2К составило 0,173 мс, что является удовлетворительным для реализации на одноплатном компьютере.

5. Заключение

Рассмотрен алгоритм обнаружения саботажа для систем видеонаблюдения, работа которого является эффективной, и обеспечивается режим реального времени на одноплатном компьютере. Определены необходимые константы для корректной работы на основе обработки ряда видеопоследовательностей. Тестирование выполнено на одноплатном компьютере Raspberry Pi 4B.

Рис. 2. Изображения из тестового набора:
а-в – исходные видеокадры; *г-е* – объектив перекрыт объектом светлого цвета;
ж-и – объектив перекрыт объектом темного цвета

Библиографические ссылки

1. *Топольский Н. Г., Демехин Ф.* Комплексная оценка эффективности автоматизированных систем противопожарной защиты предприятий нефтепереработки с использованием видеотехнологий // Безопасность жизнедеятельности. 2009. № 4. С.33–36.

2. Разработка аппаратно-программного комплекса дистанционного обнаружения пожаров / Л. В. Катковский [и др.] // Технологии безопасности. 2012. № 1. С. 43–45.

3. Attacks and Preventive Measures on Video Surveillance Systems: A Review / P. Vennam [et al.] // Applied Sciences. 2021. Vol.11, № 12. P. 5571.

4. *Wang Y. K.* Real-time camera anomaly detection for real-world video surveillance // Proceedings of the International Conference on Machine Learning and Cybernetics. 2011. P. 1520–1525.

5. Automated camera dysfunctions detection / S. Harasse [et al] // Proceedings of the 6th IEEE Southwest Symposium on Image Analysis and Interpretation. 2004. P. 36–40.

6. Implementation of an Outdoor Camera Sabotage Detection System Model / Kodithuwakku Y. [et al] // Proceedings. of the IEEE International Conference on Advanced Systems and Emergent Technologies (IC_ASET). 2024. P. 1–6.

7. *Adamovskiy Y., Bohush R.* Real-Time Algorithm for Light Gray Smoke Detection in Video Sequences // 8th International Conference on Computing, Control and Industrial Engineering (CCIE2024). Lecture Notes in Electrical Engineering, 2024. Vol. 1252. P. 535–542.