СПЕЦИФИКА ОРГАНИЗАЦИИ СИСТЕМ ВИДЕОНАБЛЮДЕНИЯ В АЭРОПОРТАХ

Любой крупный объект – отдельная категория для обеспечения безопасности. Особенно актуальной становится задача гарантии безопасности для мест, характеризующихся большим скоплением людей. К данной категории объектов по праву могут быть отнесены аэропорты.

Задачи, решаемые системой видеонаблюдения в аэропорту, во многом аналогичны задачам наблюдения на каком-либо крупном объекте, где существуют большие скопления людей. У аэропорта есть проходные, периметр, парковки, подсобные помещения и т. п., наблюдение за которыми, зачастую, важнее, чем наблюдение за людьми, находящимися непосредственно в «чистых» и «грязных» зонах на территории самого аэропорта. Основной целью комплекса мер по обеспечению безопасности должно являться недопущение вооруженных или агрессивно настроенных лиц. Подобный подход соответствует общему правилу о том, что гораздо проще и важнее предупредить правонарушение, чем ликвидировать его последствия. Следует отметить, что идентифицировать правонарушения непосредственно в толпе сложнее, чем выявить потенциальных правонарушителей во время прохождения индивидуального досмотра. В связи с этим система видеонаблюдения должна обеспечивать эффективный контроль периметра объекта, входов, проходных и прилегающей территории.

При обеспечении безопасности в аэропорту приоритетным является эффективное взаимодействие операторов системы видеонаблюдения и сотрудников службы безопасности. Поэтому система видеонаблюдения должна использоваться совместно с системой внутренней связи, обеспечивая тем самым эффективное реагирование. Операторы системы безопасности должны иметь быстрый и удобный доступ к графическим планам объекта для оперативного ориентирования. Современная программная платформа для систем безопасности – программное обеспечение (ПО) Honeywell WINMAG предоставляет доступ к трехмерным графическим планам, что повышает удобство использования. Возможно не только отображение трехмерных планов с динамическими пиктограммами, но и создание сценариев графической визуализации. Важно помнить, что угрозы безопасности могут исходить не только от действий людей, но также могут быть связаны с внештатными ситуациями (пожар, задымление). Также одной из угроз может стать проникновение посторонних лиц в подсобные помещения. Для того, чтобы обнаружить угрозы такого плана, необходимо использовать комплексную интегрированную систему безопасности, включающую в себя не только систему видеонаблюдения, но и СКУД, и систему пожарной сигнализации.

Важно, чтобы программное обеспечение системы позволяло качественно визуализировать события от различных подсистем. ПО WINMAG предоставляет возможность свободного программирования средств визуализации и реагирования системы на события. Оно предоставляет полнофункциональную интеграцию с адресно-аналоговыми пожарными системами ESSER by Honeywell, IP-системы видеонаблюдения MAXPRO VMS и обеспечивает открытые интерфейсы для интеграции систем сторонних фирм-производителей через протоколы OPC и BACnet.

Интеллектуальный анализ видеоизображений является одним из наиболее быстро развивающихся направлений. На современном рынке представлены различные решения по видеоанализу для наблюдения за местами скопления людей. Многие компании-производители подобных систем приписывают своим решениям нереализуемые функциональные возможности, что в результате приводит к разочарованию со стороны заказчика. Среди таких «функций» можно отметить обнаружение оставленных предметов (данная функция хорошо работает лишь в некоторых идеальных условиях) и «анализ» поведения людей в толпе (задачи этого класса плохо формализуются при разработке алгоритмов, что приводит к низкой эффективности автоматизации процесса принятия решений). Большинство реально используемых систем видеоаналитики способны эффективно выявлять только несколько типов действий. В общем случае некорректными или потенциально опасными могут быть следующие действия:

- Классическое обнаружение движущихся людей в запрещенных зонах.
- Обнаружение людей, двигающихся в «неправильном» направлении. Например, пытающихся выйти через область входа или движущихся в зоне таможенного или паспортного контроля в обратном направлении.
- Обнаружение людей, двигающихся с нестандартной скоростью. К примеру – бегущий по залу человек может пытаться скрыться от службы охраны.
- Обнаружение людей или предметов, находящихся в контролируемой зоне свыше установленного интервала времени. Эта функция может быть полезна, скажем, при охране автомобильных парковок. Обычно люди находятся там непродолжительное время, в течение которого они осуществляют посадку и высадку из автомобиля. Если же человек ходит по парковке в течение длительного времени, это может оказаться подозрительным.
- Обнаружение людей, находящихся в контролируемых зонах вне разрешенного времени.
- Регистрация прохода через маршруты ограниченного доступа, например, через пожарные или служебные выходы.

- Перемещение объектов или субъектов из зон свободного доступа в запрещенные зоны или через границы таких зон. В качестве примера можно привести проникновение посторонних лиц в автомобильные или железнодорожные тоннели – очевидно, что при этом система не должна реагировать на движущиеся автомобили и поезда.
- «Неправильная» траектория движения автотранспорта. Например, поворот или разворот в запрещенном месте.

Упомянутые действия в определенных ситуациях могут либо быть несанкционированными, либо предшествовать им, либо предшествовать опасной ситуации. Самый важный результат внедрения видеоаналитики состоит в том, что служба безопасности сможет реагировать на потенциально опасные действия на более ранних стадиях, а не после того, как инцидент уже произошел. Видеоаналитика по распознаванию автомобильных номеров оказывается весьма эффективной при контроле парковок и въездов автотранспорта.

Система с функциями видеоанализа может использоваться не только при наблюдении за объектом в реальном масштабе времени, но и для анализа уже сделанной видеозаписи. Например, если требуется найти все видеофрагменты, содержащие определенный вид действий людей в кадре. Очевидно, что ручной поиск событий (каждое из которых может занимать несколько секунд) в многочасовой видеозаписи выполнить крайне сложно. Даже если поиск осуществляется с использованием видеообнаружителя движения. Особенно при большом числе телекамер. Поэтому при выборе системы с функциями видеоанализа стоит обратить внимание на возможность использования записи в качестве исходного материала для анализа. Необходимо также, чтобы оператор мог самостоятельно настроить события, по которым осуществляется поиск.

Стоит отдельно остановиться на такой функции видеоаналитики как распознавание лиц. Лицо человека не является стационарным объектом и может существенно изменяться за сравнительно небольшой промежуток времени под действием эмоций, грима, макияжа, а также за счет появления или удаления новых элементов, таких как очки, усы или борода. Кроме этого, оно является трехмерным объектом, изображение которого зависит от угла зрения, яркости и спектральных составляющих падающего света. Большинство применяемых в настоящее время алгоритмов идентификации по геометрии лица используют характерные ключевые точки на лице и взаимные расстояния между ними. Задача выделения характерных деталей лица хорошо решается только для плоских двухмерных изображений с фронтальной подсветкой. Не стоит забывать, что лицо человека может быть закрыто маской, используемой, например, для защиты органов дыхания от загрязненного воздуха или инфекций. Маска может скрывать лицо почти полностью, не позволяя выполнить идентификацию по изображению. В связи с этим применение системы распознавания лиц на объектах с массовым скоплением людей для выявления преступников оказывается неэффективным.

В настоящее время основной прогресс в области распознавания лиц связан с применением искусственных нейронных сетей (нейросетей). Идея нейросетей заключается в том, чтобы смоделировать работу человеческой нервной системы – а именно, ее способности к обучению и исправлению ошибок. В этом состоит главная особенность и преимущество нейросети перед традиционными алгоритмами – она способна действовать на основании предыдущего опыта, с каждым разом делая все меньше ошибок. В процессе обучения нейронная сеть способна выявлять сложные зависимости между входными и выходными данными. Это значит, что в случае успешного обучения сеть сможет вернуть корректный результат на основании неполных или искаженных данных, а иногда, и данных, отсутствовавших в исходной (обучающей) выборке. Применительно к видеонаблюдению нейросети оказались эффективным средством для распознавания образов. Почему данная технология появилась только сейчас, ведь нейросети были известны с 40-х годов прошлого века? Этому способствовало несколько факторов. Во-первых, появился большой и общедоступный массив изображений, на которых можно обучаться. Во-вторых, современные видеокарты (GPU), содержащие тысячи простых процессоров, позволяют эффективно распараллеливать процессы, необходимые для обучения и работы нейросетей. В-третьих, появились готовые нейросети и новые эффективные методы обучения, распознающие образы, на основании которых можно делать свои приложения. Нейросети и машинное обучение сегодня возглавляют рейтинг самых востребованных технологий.

Стоит отметить, что при защите объектов, связанных с большим скоплением людей, необходимо решать проблему обеспечения безопасности комплексно. Существенное увеличение надежности обнаружения угроз объекту в комплексных и интегрированных системах безопасности достигается за счет использования нескольких подсистем для обнаружения одной и той же угрозы (несанкционированное проникновение на объект может регистрироваться подсистемами охранной сигнализации и видеонаблюдения). Кроме этого, использование интегрированной системы оказывается более целесообразным с экономической точки зрения по сравнению с внедрением и эксплуатацией нескольких отдельных систем за счет использования общих средств сбора, обработки и управления информацией.

Сейчас на рынке присутствует множество компаний, предлагающих «интегрирующие» программные продукты для систем безопасности, позволяющие осуществлять мониторинг и управление оборудованием различных фирм-производителей. Эти решения нельзя назвать интегрированными. У пользователей таких решений могут возникнуть проблемы, связанные с расширением системы, выходом обновлений и новых версий аппаратного обеспечения (поскольку оно производится сторонними компаниями), а также – с технической поддержкой от нескольких независимых компаний. В связи с этим полноценная интеграция возможна только для решений, выпускаемых одной компанией-производителем, имеющей достаточные ресурсы не только для написания программного обеспечения, но и выпуска полного функционального ряда оборудования.

Подводя итог, стоит отметить, что только в случае, когда все элементы интегрированной системы изначально разрабатываются с учетом дальнейшего полноценного взаимодействия, становится практически возможным реализовать все заявленные функциональные возможности оборудования. При этом важно, чтобы компания-производитель данного решения являлась разработчиком не только программного, но и аппаратного обеспечения. Компания Honeywell является разработчиком и производителем полного функционального ряда оборудования и программного обеспечения для построения систем безопасности на базе IP-технологий. Список продуктов включает в себя IP-камеры, аналоговые, гибридные и сетевые видеорегистраторы, IP-контроллеры СКУД, контрольные панели и извещатели охранно-пожарной сигнализации, а также специализированное программное обеспечение для видеоанализа, управления видеоизображениями и создания комплексных интегрированных систем безопасности. Именно в этом состоит уникальность предлагаемых Honeywell решений, поскольку все элементы изначально разрабатываются с учетом полноценной интеграции.

Honeywell

THE POWER OF **CONNECTED**

АО «ХОНЕВЕЛЛ»
121059, Москва, ул. Киевская, д. 7
тел.: (495) 797-9371, (495) 796-9800
191123, Санкт-Петербург,
ул. Шпалерная, д. 36
тел.: (812) 329-5722
e-mail: securityrussia@honeywell.com
www.security.honeywell.com/ru