Khoroshilov Aleksey Yurievich
student
Scientific adviser
Fomicheva Tatyana Leonidovna
candidate of economics sciences, associate professor
ФГОБУ ВО «Финансовый университет
при Правительстве Российской Федерации»
Moscow
Хорошилов Алексей Юрьевич
бакалавр, студент
Научный руководитель
Фомичева Татьяна Леонидовна
канд. экон. наук, доцент
ФГОБУ ВО «Финансовый университет
при Правительстве Российской Федерации»
г. Москва

DOI 10.31483/r-99746

PROSPECTS FOR SURVEILLANCE SYSTEMS USAGE

***Abstract**: the article evaluates the expansion tendency of surveillance systems, used for security and maintaining order. Related risks are analyzed.*

***Keywords**: surveillance, privacy, face recognition, information security.*

ПЕРСПЕКТИВЫ ИСПОЛЬЗОВАНИЯ СИСТЕМ ВИДЕОНАБЛЮДЕНИЯ

***Аннотация**: в статье оценивается тенденция расширения систем видеонаблюдения, используемых для обеспечения безопасности и поддержания порядка. Анализируются связанные с этим риски.*

***Ключевые слова**: видеонаблюдение, конфиденциальность, распознавание лиц, информационная безопасность.*

Surveillance systems are spreading dramatically around the world due to being used in surveillance and maintaining order. Programs embedded are capable of face recognition, according to the recent research the face recognition per cent in China was 99,8%. Nevertheless, COVID-19 pandemic had its influence on the program development due to people wearing masks in public places. Yet, the recognition percentage remained high – about 98%. Furthermore, programs are capable of capturing traffic violation, identifying people's mood, recognizing the unusual behavior. Cameras are the key issue standing behind the «Crime drop» because with its invention committing a crime without the risk of being caught has dramatically dropped.

Neural networks were the cause of cameras expansion as well. The reason is that average human starts to miss 45% of potential threats after 12 minutes of close supervising, what demands surveillance systems to be embedded with the analysis system, which could help people to supervise 24 hours a day. Nevertheless, we cannot fully rely on analysis systems as they have their own drawbacks such as crashes, glitches, system failures, under the influence of weather analysis system can be distorted, etc.

However, there is some more important issue to take into consideration: how can we avoid observers abusing surveillance? Every person can be tracked on a regular basis. Moreover, information analysis in this case may lead to information leaks of individual's data involving home, work and study locations, health issues, etc. Even if we trust the law enforcement authorities to protect our personal information, there still are observers, who can abuse their powers. Special privacy-preserving protocols, which are created to protect personal information from leaking, are not enough. Therefore, there are two ways of solving the problem:

1. Limit the time and location access to cameras.

2. Limit what can be seen in the individual frames.

In the first case, for example, observer can have access only to those cameras that are installed in a kilometer radius within his location or can gain access to cameras only in his official work time. In the second one field of view is limited based on the high-level semantic information obtained from the content of the video stream, that way observer will not have limitless access to the data, as he will only be able to watch the

data similar to the semantic content of what he is allowed to watch. The second case is more flexible and suitable for observer in comparison with the first one dealing with physical context. Still, observer can see extra information. For instance, police officer can watch recordings, where some car sped up. In that scenario he is interested only in the registration car number, however, he can see all the people in the car or the nearby cars while the only one of them is breaking the law. These two approaches do not exclude each other and can be used together as some kind of hybrid.

Besides, we should not forget about hackers. They can hack into cloud or can gain access to cameras and their analysis system as well. Moreover, what if they hack the analysis system and use synthetic media such as Deepfakes, Faceswap or DeepfaceLab in order to swap the face of the person committing crime? Currently these programs are not perfect and skilled IT expert can spot these kind of manipulations but technology is progressing and this makes a serious concern about the future evidence faking.

All related risks considered, I think that surveillance systems are worth developing, expanding in order not to leave blind spots in the city. It will help to decrease criminality and secure citizens.

Список литературы

1. Elmahdi Bentafat, M. Mazhar Rathore, Spiridon Bakiras. Towards real-time privacy-preserving video surveillance. URL: https://www.sciencedirect.com/science/article/pii/S0140366421003388

2. Govind Jeevan, Geevar C. Zacharias, Madhu S. Nair, Jeny Rajan. An empirical study of the impact of masks on face recognition. URL: https://www.sciencedirect.com/science/article/pii/S003132032100488X

3. Mattia Bonomi, Cecilia Pasquini, Giulia Boato. Dynamic texture analysis for detecting fake faces in video sequences. URL: https://www.sciencedirect.com/science/article/pii/S1047320321001553

4. Chumachenko K.K. The problem of computer vision algorithms integration in surveillance systems. URL: https://cyberleninka.ru/article/n/problemy-integratsii-algoritmov-kompyuternogo-zreniya-v-sistemy-videonablyueniya/viewer