Privacy Protection in Conditions of Use CCTV Systems

Hemin Akram Muhammad
Tomas Bata University in Zlin, Nad Stráněmi 4511, 760 05 Zlín,
e-mail: muhammad@utb.cz

Ludek Lukas
Tomas Bata University in Zlin, Nad Stráněmi 4511, 760 05 Zlín,
e-mail: lukas@utb.cz

Abstract

The main goal of this research is presenting some mechanisms used in the CCTV system for protecting personal information. Besides illustrating CCTV integration, application, and intelligent system, the research shows some solutions that are used for protecting personal information in real-time video streaming such as Respectful Cameras System (RCS), Automatic Face Masking Techniques (AFMT), and Scheiderman–Kanade Face Detector (SKFD). The advantages and disadvantages of the presented techniques are discussed, as well as guidelines and requirements of the General Data Protection Regulation (GDPR) regarding using video surveillance systems are argued.
Keywords: CCTV, GDPR, RCS, AFMT, SKFD, video surveillance

1. Introduction

The security system plays a great role in most of today's situations. A security system should cover necessities for video valuation, intrusion discovery, two-way communication, fire revealing, and access control. In most critical circumstances such as terrorism and theft, Closed-Circuit Television (CCTV) has been used effectively for protecting assets and personal. Before and in the early 1990s only analog camera system was available but after that, the Video System components changed from analog to digital imaging technology and became more friendly with computer systems. Thus, video technology now is very well developed and has become a vital part of the security solution. As a consequence of sophisticating computer components (Processor, Hard Disk, and Random Access Memory) and reducing their prices in early 2000, CCTV became more useable and dependable in security surveillance systems. CCTV has many important roles such as the role of asset protection by observing the location of assets, observing movements in monitored location, and detecting unsolicited entry into a facility by monitoring at the border or perimeter of the location [1].

On the other hand, protecting personal identity in video systems is studied by many researchers recently. After September 11th of 2001, more and more video cameras have been deployed in a variety of locations for security and monitoring purposes. Through these cameras, people's appearances and activities are recorded and stored in digital forms, which can be easily shared on the internet or in DVDs, but sharing video records to the third party without any privacy-encoding may seriously threaten people's privacy. The traditional privacy protection method in video systems is face masking which is manually blocked or blurred in video frames. Such kind of masking is not feasible because it cannot be implemented in live

video streaming and it needs more time. In contrast, recently many sophisticated video systems are offered with the power of protecting personal identity in real-time [1]-[3].

2. CCTV Integrations

Video Surveillance Systems are most actual when combined with other security hardware and procedures to form an intelligible security system. Once a video system is integrated with the other security devices the whole security system is more productive than the individual subsystems. CCTV can be integrated with electronic access control, intrusion and motion alarm sensors, fire alarm sensors, security guard personnel, and communication devices. Figure 1 shows the components integrated in a security system. Perimeter Guard System is an example of an integrated Video system. Besides of CCTV system, it contains an intrusion-detection alarm, Access control system, Safety system, and communications devices [4][6].

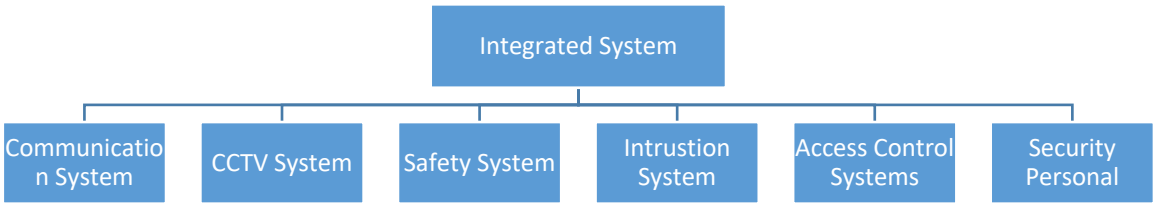

Figure 1 Integrated Security System [5]

3. CCTV and Intelligent Video Surveillance Systems

Intelligent video surveillance is a technology that records criminal activity in installed places based on the preferences of the user and it is the cutting-edge video technology. The main objectives of this system are tracking a moving target, automatic detection of suspicious activity, and alarming the operators. This technology is a part of CCTV systems which can be used for protecting personal privacy and which can assist operators to control more cameras and respond faster. Additionally, the construction of an intelligent video system can be centralized or distributed. In a centralized architecture, all intelligence exists in the recording server as showed in figure 2. This means that server functions as an open platform which makes adding functions easier [5].

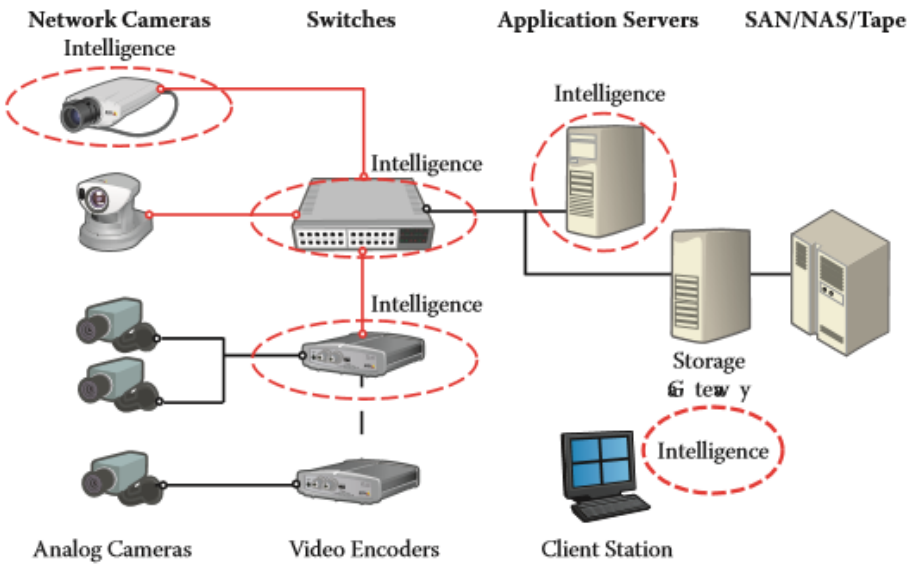

Figure 2 Intelligent Video Surveillance System [3]

In a distributed system, the intelligence is distributed to the edge and exists in the network camera, and analysis is done locally in the camera. Usually, video intelligence is a necessity in systems where a fast reply time is requested or a very large number of cameras are to be managed proactively [3].

4. CCTV System and Privacy Protection

In today's era, a varied range of cryptographic techniques and security systems have been used to protect sensitive personal information. But these methods cannot be straightly used for privacy protection of imagery data, they usually work well for textual and categorical information. Current common deployment and increased complexity of video surveillance systems have raised the anxiety of their threat to individuals' right to privacy. In video surveillance systems, there are three major tasks to privacy protection. The first one is to detect the privacy information needed to be conserved. The next step is to define a suitable video modification method that can be used to secure privacy. In the final step, privacy data management needs to be invented to manage private information. According to [7] the privacy protection system should contain the following five objectives:

1. Privacy: a protected data or video should not provide any information on whether a specific user is in the scene.
2. Usability: A protected video has to be avoided from visible objects that are offered during video processing.
3. Security: video data should be presented at computing units that possess suitable permission.
4. Accessibility: A user can have the ability to prohibit a client's access to his/her protected data.
5. Scalability: The architecture should be scalable to many cameras and should be away from a single point of failure.

5. Privacy Protection Models in CCTV Systems

Nowadays, people's appearances and movements are digitally recorded and stored via video cameras since video cameras are installed in many places for security and monitoring purposes. Stored data creates a threat to personal privacy because it can be shared easily without masking or any consideration. The traditional way of protecting privacy was masking faces manually by blurring or blocking subjects in video frames. This method was not easy, required more time, not applicable to real-time video, and high-cost processes. Thus, it is very difficult to protect a long video traditionally. Therefore, many researchers are interested in producing an automatic technique for protecting personal information in the video surveillance system. The following are some models produced for protecting personal information[8].

Respectful Cameras System: this system is A real-time method that can detect movements for concealing individual identities. In this system people who demand to remain unidentified wear colored markers such as hats or vests. The system follows these markers automatically using statistical learning and classification to conclude the location and size of each face. It conceals faces with solid ellipsoidal overlays. The method depends on some functionalities such as a visual color-tracker, 9D color-space, Probabilistic Adaptive Boosting (AdaBoost) classifier, Sampling Importance Resampling (SIR), and Particle Filtering to incorporate inter-frame temporal information. As the system depends on visual markers worn by individuals, therefore, the input of the system is the sequence of images from a video stream. Figure 3 shows two video frames, the left frame is the input frame to the system while the right frame is the output frame of the system which elliptical overlay ides the face of a man who wore a green vest. As the Respectful cameras system trained to detect green vests. [9]

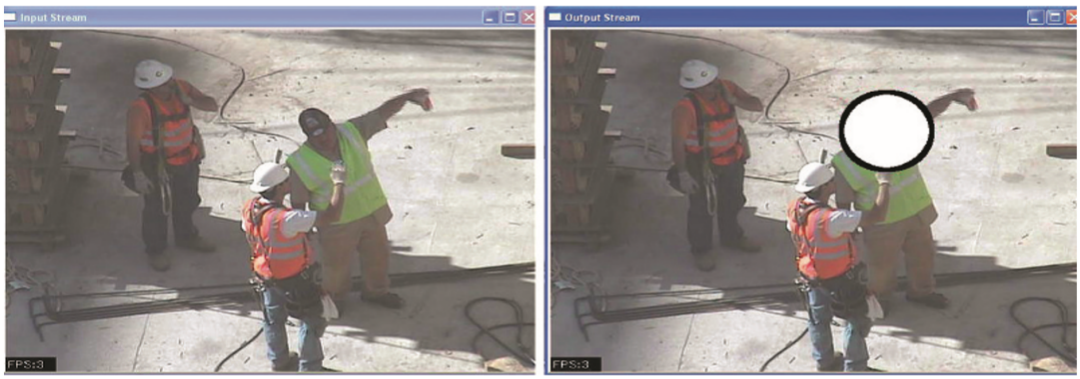

Figure 3 Sample video with Respectful Camera System [5]

Automatic Face Masking: this technique automatically identified a person by face recognition, and displayed a silhouette image of the person with a name list to balance privacy-protection and information-conveyance. It is relaying on detecting and tracking faces in video frames then produces obscuring masks by using the detected face locations and scales as shown in figure 4. Face detection can be obtained by many visual features such as shape, color, texture, and appearance [10].

Figure 4 Sample video with Automatic Face Masking [5]

Schneiderman–Kanade face detector: This detector works perfectly in detecting faces in video records. It depends on face tracking that improves face detection. This technique follows an individual's head or facial features over a video image sequence by using sequential correspondences between frames. Besides face detection and tracking, it relays on an algorithm called bi-directional tracking algorithm which combines face detection, tracking, and background subtraction. Firstly, extract the foreground by subtracting the background then face detection obtained on the foreground. Then the face is tracks simultaneously in both backward and forward directions as shown in figure 5[10].

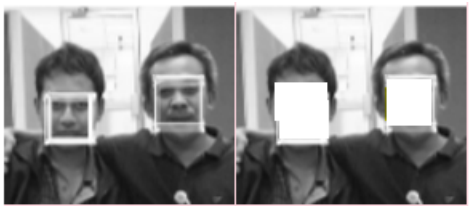

Figure 5 Sample video Schneiderman-Kanade Face Detector [5]

Prototype: for protecting privacy is designed for a multi-camera video system environment. It depends on real-time human tracking RFID systems to detect individuals. The RFID system sends the information to each camera that segments, tracks, identifies, and removes visual objects that match individuals with RFID tags. To repair the rest of the video, an object-based video inpainting algorithm is employed to fill in the unfilled regions and produce the protected video [7].

6. Conclusion

Closed-Circuit Television (CCTV) plays a great role in protecting human's life and assets. It has two main types which are analog and digital image technology. Nowadays the digital type is more common and usable. CCTV has many applications and they are used in different situations for different purposes. Since it is used in many places and covers many views, people's appearances and activities are recorded. Protecting personal identity is very necessary therefore many technics are using but each of them has its specification. Most of the techniques are focused on face masking. Each technique has some specialty in forming and using algorithms, for example, the Respectful Camera System is based on a model that can conceal people's activity during movement in a real-time video covering but the system depends on a visual marker that should be worn by the individuals while Automatic Face Masking Technique depends on tracking faces in video frames where the faces are blurred with colors. Concerning theses technics, CCTV should be used according to the regulations such as GDPR that are accepted by European countries.

Moreover, Privacy protection in the CCTV system is an interesting area by developers. Building privacy protection technique in CCTV not easy and face some challenges. In general, most of the currently developed techniques consist of three different phases. In the first phase, after recognizing the individuals whose privacy needs for protection, an algorithm is applying to delete the individuals' images. Then in the second phase, a scheme is used to insert the extracted private information into a modified video. But the scheme let the original data to be retrieved with proper verification. Third, the original video can store as private assets of the individuals in a secure infrastructure system that permits individuals to selectively grant access to their private information. The offered systems suffer from many failures such as sensor failure, segmentation failure, and issues in algorithms. Happening these failures in a single video frame leads to the defeat the entire system. However, the systems perform well in a controlled area with fixed lighting but most of them cannot work fine with outside area lighting.

7. Reference

1. Kruegle, H. (2007). CCTV Surveillance Analog and Digital Video Practices and Technology. *Elsevier*.
2. Andrew, S.,Arun, H., Sharath, P., Yingli, T., Lisa, B., Ahmet, E., Jonathan, C., Chiao-Fe, S., Max, L. (2003). Enabling Video Privacy through Computer Vision. *IBM Research Report*.
3. Silhavy, P., Silhavy, R., Prokopova, Z., Kominkova, Z. (2015). Intelligent Systems in Cybernetics and Automation Theory. *Springer, Vol 2.*
4. Tansuriyavong, S. and Shin-ichi, H. (2001). Privacy Protection by Concealing Persons in Circumstantial Video Image. *In Proc. of PUI*.
5. Senior, A. (2009). An Introduction to Automatic video Surveillance. *Springer*.
6. Hromada, H., Lukas, L. (2012). Critical Infrastructure Protection and the Evaluation Process. *IJDRBC*, Vol3.
7. Andrew, S. (2009). Protecting Privacy in Video Surveillance, *Springer*.
8. Cheung, SC., Venkatesh, M., Paruchuri, J., Zhao, J., Nguyen, T. (2009). Protecting and Managing Privacy Information in Video Surveillance Systems. *Springer*.
9. Jeremy, S., Marci, M., Deirdre, K., Shankar, S., Ken, G. (2009). Respectful Cameras: Detecting Visual Markers in Real-Time to Address Privacy Concerns. *Springer*.
10. Datong, Ch., Yi, Ch.,Rong, Y., Jie, Y. (2009). Protecting Personal Identification in Video, *Springer*.