View metadata, citation and similar papers at core.ac.uk
brought to you by CORE
provided by Institute of Advanced Engineering and Science

International Journal of Electrical and Computer Engineering (IJECE)
Vol. 8, No. 4, August 2018, pp. 2072~2082
ISSN: 2088-8708, DOI: 10.11591/ijece.v8i4.pp2072-2082

CCTV Surveillance System, attacks and design goals

Muthusenthil B[1], Hyun sung Kim[2]
[1]Information Security Research Institute, Wookyoung Information Technology Dongbuk-ro, Buk-gu, Daegu, Korea
[1]Valliammai Engineering College, Chennai, Tamilnadu, India
[2]Hyung Sung Kim Department of Cyber Security, Kyungil University Korea, Korea

Article Info

Article history:

Received Oct 4, 2017
Revised Feb 22, 2018
Accepted Mar 1, 2018

Keyword:

Attacks
Criminal investigations
Design rules
Intrusiveness
Surveillance systems
Video processing systems

ABSTRACT

Closed Circuit Tele-Vision surveillance systems are frequently the subject of debate. Some parties seek to promote their benefits such as their use in criminal investigations and providing a feeling of safety to the public. They have also been on the receiving end of bad press when some consider intrusiveness has outweighed the benefits. The correct design and use of such systems is paramount to ensure a CCTV surveillance system meets the needs of the user, provides a tangible benefit and provides safety and security for the wider law-abiding public. In focusing on the normative aspects of CCTV, the paper raises questions concerning the efficiency of understanding contemporary forms of 'social ordering practices' primarily in terms of technical rationalities while neglecting other, more material and ideological processes involved in the construction of social order. In this paper, a 360-degree view presented on the assessment of the diverse CCTV video surveillance systems (VSS) of recent past and present in accordance with technology. Further, an attempt been made to compare different VSS with their operational strengths and their attacks. Finally, the paper concludes with a number of future research directions in the design and implementation of VSS.

Copyright © 2018 Institute of Advanced Engineering and Science.
All rights reserved.

Corresponding Author:

Muthusenthil B,
Information Security Research Institute,
Wookyoung Information Technology,
Dongbuk-ro, Buk-gu, Daegu, Korea.
Email: bmssen@gmail.com

1. INTRODUCTION

CCTV (Closed Circuit Tele-Vision) is one of the most widely used physical security technologies. A surveillance camera is a video collection device installed at a particular location and utilized for a variety of purposes. As CCTV performance has become enhanced recently, technology is being developed that attempts to perform automated processing through facial recognition using the facial information acquired from a CCTV system [1]-[5]. However, if these technologies are exploited maliciously, privacy may be seriously violated. A set of communication equipment devices that collect image information from a surveillance camera device installed at a particular location, and transmit the images via an opened wire/wireless communication channel, so that only specified persons can receive it [6].

a. Image monitoring control server

A server that stores, manages, and monitors the image information received from a surveillance camera. The image monitoring server is composed of several modules such as encryption, decryption, facial area detection, privacy protected image, image saving, and monitoring. The monitoring module can be located behind the en/decryption module or privacy protected image module, depending upon whether privacy protection is to be applied or not, while monitoring the image [7], [8].

b. Client

A system or user that seeks to receive and use the CCTV image from the image monitoring and control server. Desktops, laptops, and mobile phones can be an example of clients. The client is composed of the en/decryption, facial recognition, and image utilization modules [16].

c. Facial Area Detection

A process that must be executed before recognizing the face, and which detects the image spot where the face is located. Generally speaking, "facial area detection" refers to the phase that identifies major facial parts such as the face shape, eyes, nose, and mouth, whereas the "characteristics extraction phase" refers to pre-processing after facial area detection, as well as facial feature extraction for the face area [14], [15].

Our goal in this paper is to provide a clear overview of various video survelliance system (VSS) suggested by various researchers and provide a guide for further design and development in this area. The contributions of our work are listed as follows:

1. We summaries the various categories of VSSs.
2. We classify the current state of VSS and outline several major open attacks are possible in VSS.
3. We provide design goals for the development of future VSS which can be integrated into existing VSSs.

This paper is organized as follows. Section 2 gives an overview of various VSSs. Section 3 we review main attacks taxonomies for video surveillance systems. Section 4 provides we provide a set of recommendations that can help improve the design and development, which includes security and privacy levels provided by the hardware, the firmware, the network communications and the operation of video surveillance systems. Section 5 concludes our work.

1.1. Overview of surveillance system

a. CCTV Systems

With the development of the Internet network, the network based CCTV is now widely used in our society. In particular, CCTV is used for crime prevention, and the scope of utilization is gradually expanding.

Video cameras are either analogue or digital, which means that they work on the basis of sending analogue or digital signals to a storage device such as a video tape recorder or desktop computer or laptop computer [9], [10].

b. Analogue

Can record straight to a video tape recorder which are able to record analogue signals as pictures. If the analogue signals are recorded to tape, then the tape must run at a very slow speed in order to operate continuously. This is because in order to allow a three-hour tape to run for 24 hours, it must be set to run on a time lapse basis which is usually about four frames a second. In one second, the camera scene can change dramatically. A person for example can have walked a distance of 1 meter, and therefore if the distance is divided into four parts, i.e. four frames or "snapshots" in time, then each frame invariably looks like a blur, unless the subject keeps relatively still [11]-[13].

c. Digital

These cameras do not require a video capture card because they work using a digital signal which can be saved directly to a computer. The signal is compressed 5:1, but DVD quality can be achieved with more compression (MPEG-2 is standard for DVD-video, and has a higher compression ratio than 5:1, with a slightly lower video quality than 5:1 at best, and is adjustable for the amount of space to be taken up versus the quality of picture needed or desired). The highest picture quality of DVD is only slightly lower than the quality of basic 5:1-compression DV [17]-[19].

d. Network

IP cameras or network cameras are analogue or digital video cameras, plus an embedded video server having an IP address, capable of streaming the video (and sometimes, even audio). Because network cameras are embedded devices, and do not need to output an analogue signal, resolutions higher than closed-circuit television 'CCTV' analogue cameras are possible. A typical analogue CCTV camera has a PAL (768×576 pixels) or NTSC (720×480 pixels), whereas network cameras may have VGA (640×480 pixels), SVGA (800×600 pixels) or quad-VGA (1280×960 pixels, also referred to as "megapixel") resolutions.

e. Digital still cameras

The pixel resolution of the current models has easily reached 7 million pixels (7-mega pixels). Some point and shoot models like those produced by Canon or Nikon boast resolutions in excess of 10 million pixels.

At these resolutions, and with high shutter speeds like 1/125th of a second, it is possible to take jpg pictures on a continuous or motion detection basis that will capture not only anyone running past the camera scene, but even the faces of those driving past. These cameras can be plugged into the USB port of any

computer (most of them now have USB capability) and pictures can be taken of any camera scene. All that is necessary is for the camera to be mounted on a wall bracket and pointed in the desired direction [18].

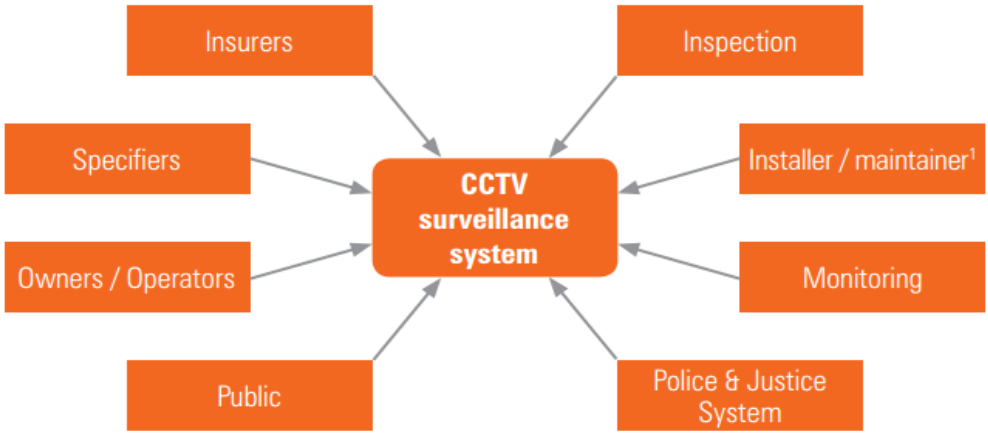

Figure 1. CCTV Surveillance System

As shown in Figure 1, the CCTV system is composed of various wire/wireless surveillance cameras connected to an image monitoring control server, as well as the client [19]. The CCTV system transmits and receives image data via a wire/wireless communication channel, as is composed of various components, such as the surveillance camera, image monitoring control server, authentication and access control server, mobile phone, desktop, and laptop.

2. OVERVIEW OF VIDEO SURVEILLANCE SYSTEM AND CATEGORIES

In this section, we review relevant literature on CCTV System and various categories of video surviellance systems.

2.1. CCTV system

CCTV-based surveillance networks are widely used for security in public places. An important installation problem is to assign a camera schedule with which the system can choose which camera to record its video frames to storage at a certain time. Because of the resource constrained and bandwidth limitation, only a subset of raw video frames can be recorded for a camera. For security concerns, it is expected that the captured frames from the same camera should have equal temporal distance between any two successive ones. If all the distances are not the same, there is jitter. Kuan Jen Lin *et al*. [17] have developed the formulation of the scheduling problems is presented. Furthermore, efficient scheduling algorithm is proposed to find feasible schedules given a jitter bound. Experimental results show the efficiency and practicability of the proposed algorithms.

Efficiency and robustness are the two most important issues for multi object tracking algorithms in real-time intelligent video surveillance systems. We propose a novel approach to real-time multi object tracking in crowds, which is formulated as a maximum a posteriori estimation problem and is approximated through an assignment step and a location step. Observing that the occluding object is usually less affected by the occluded objects, sequential solutions for the assignment and the location are derived. A novel dominant color histogram (DCH) is proposed as an efficient object model.

The DCH can be regarded as a generalized color histogram, where dominant colors are selected based on a given distance measure. Comparing with conventional color histograms, the DCH only requires a few color components (31 on average). Liyuan Li *et al*. [18] have proposed multi object tracking method is based on a generalized color histogram a novel DCH that is shown to be robust to color and brightness changes. The proposed assignment step includes the estimation of orders of visibility, sequential assignment, and exclusion. The proposed location step contains visible order estimation, sequential operations of mean-shift location, and exclusion. Our tests on a large number of videos and real CCTV systems showed that the proposed method is able to track multiple objects through crowds in a high rate of success.

Ming Ying *et al*. [19] have suggested that the visual design method should be introduced and advantages of spatial analysis and information query of GIS and 3D city model should be fully used to aid CCTV monitoring system in design and maintenance.

Pradeep K. Atrey *et al*. [20] have attempted to solve the problem of dynamically selecting and scheduling the four best CCTV views. We adopt a human-centric approach in which the system computes the operator's attention in the CCTV views to automatically determine the importance of events captured by the respective cameras. The experiments show that the proposed method helps a human operator in identifying important events occurring in the environment.

Roy Coleman *et al*. [21] have concerned to chart the establishment and uses of CCTV within the location of Liverpool city center. In doing this the paper seeks to contextualize CCTV within contemporary 'partnership' approaches to regeneration which are reshaping the material and discursive form of the city. Thus CCTV schemes along with other security initiatives are understood as social ordering strategies emanating from within locally powerful networks which are orderly regeneration projects. In focusing on the normative aspects of CCTV, the paper raises questions concerning the efficiency of understanding contemporary forms of 'social ordering practices' primarily in terms of technical rationalities while neglecting other, more material and ideological processes involved in the construction of social order.

Tae Hyung *et al*. [22] have examined the next generation functions and usages from the experience from the disaster and safety management system, especially CCTV, in Gimpo Smartopia, Korea. and used new hybrid methodology to rebuild requirements and design concepts in terms of their functions, service types, usages gated ratings. Based on the examination results, this paper suggested sketched the architecture and assessed implications and considerations for the public application development in the disaster and safety management.

Young-Jin Han *et al*. [23] have proposed a security framework that protects personal information obtained from the detected facial area. We pointed out the security threats within CCTV system, and then propose a counter measures. The key point of this framework is processing the mosaic or scrambling methods to the facial area, so that the facial information cannot be directly obtained without knowledge of the secret key. When the original facial information is needed, such as crime investigation, it can be obtained through reverse scrambling. This framework will contribute to protect privacy and develop the biometric-based physical security technology area.

Sergio Saponara *et al*. [24] have proposed to exploit the on-board closed circuit television (CCTV) security system to enable advanced services not only for surveillance, but also for safety, automatic climate control, e-ticketing. The new system has minimal hardware and installation cost overheads, since it exploits the already installed CCTV cameras. In addition, for each wagon, an embedded acquisition and processing node (EAP) is used, composed by a video multiplexer, and by a digital signal processor that implements algorithms for advanced services such as: smoke detection, to give an early alarm in case of a fire, or people detection for people counting, or fatigue detection for the driver. The information is then transmitted from each EAP node to the train information system. The final terminals can be the tablets of the train staff, and/or visualization displays in each wagon in case of fire alarms for the passengers.

2.2. Network based video surveillance system

Hoang Thanh Nguyen *et al*. [25] have presented a systematic approach by detailing the design, implementation, and evaluation of a large-scale wireless camera network, suitable for a variety of practical real-time applications. We take into consideration issues related to hardware, software, control, architecture, network connectivity, performance evaluation, and data-processing strategies for the network. We also perform multi objective optimization on settings such as video resolution and compression quality to provide insight into the performance trade-offs when configuring such a network and present lessons learned in the building and daily usage of the network.

2.3. Security based surveillance system

Anabham Bhavani *et al*. [26] have focused on the design and implementation of a low cost smart security camera with night vision capability using Raspberry Pi (RPI) with PIR. The system was designed to be used inside a warehouse facility. It has human detection and smoke detection capability that can provide precaution to potential crimes and potential fire. The credit card size Raspberry Pi (RPI) with A passive infrared sensor (PIR sensor) handles the moving body, control algorithms for the alarms and sends captured pictures to user's email via Bluetooth. As part of its alarm system, it will play the E-speech sounds: "intruder" when there is detection. The system uses ordinary webcam but its IR filter was removed in order to have night vision capability. With help of LDR it will sense whether it is night or day if it is night the led will on when it detect intruder.

Sonali Hargude *et al*. [27] have developed the abandoned object detection system. This paper describes methodology for Intelligent Surveillance system. Proposed Real time abandoned object detection System helps to reduce harms causing due to unattended objects. In this paper, we have covered a detail discussion on the various stages of any abandoned object detection technique. As future enhancement we can take live video feed through android mobile. As everyone is using Smartphone it will be easier to have quick looked at the system though android application. It will provide flexibility to the user or the authorized person who can keep watch from a distance.

Grigore M. Havârneanu *et al*. [28] have covered at least five relevant issues which significantly contribute to the prevention of railway suicide and trespass, and mitigation practice: (1) collating details across a wide range of countries of what is happening in terms of prevention, data on incidents and processes for investigation and the management of suicide and trespassing incidents, etc.; (2) developing and using methodology for the evaluation of extensive sets of measures; (3) providing recommendations for further examination of selected preventative measures; (4) looking for additional empirical support for a sample of selected measures; and (5) providing a toolbox with guidance materials and best practice examples to help IMs and RUs implement measures more effectively tailored to their specific needs.

S.Naga Jyothi *et al*. [29] have proposed the real time security surveillance system using IoT. The system design uses Motion Detection algorithm written in Python as a default programming environment. This significantly decreases the storage usage and save investment cost. The algorithm for Motion Detection is being implemented on low processing power chip Raspberry pi 2 and Pi camera, which enables live video streaming with detection of moving objects and g*et al*arm when motion is detected and sends photos, videos to a cloud server directly using pi camera. When cloud is not available then the data is stored locally on raspberry pi and sent when the connection resumes. The camera is mounted on the motor and its movement (Left/Right) is controlled through IoT webpage by the user, thus providing user with enhanced view of the surroundings.

Patricia Marie L *et al*. [30] have presented the design and construction of a system consisted of five mobile robots (mobots) and a communications system that will serve as a security surveillance system. This is implemented using a microcontroller as the core that enables the mobots to work cooperatively. The mobots are free to move within their designated areas and are capable of relaying messages via ZigBee communication to a base controller system. The purpose of this system is to have an alternative or even a complement to regular CCTV surveillance, especially in buildings with several rooms. This would enhance the security as the system utilizes a database to store the information gathered from intruder alerts. Furthermore, the communication radios used transmit with low power over a long range. The mobots are enabled to relay data via mobot-to-PC and mobot-to-mobot paths up to five hops. The data transmitted allows the base controller system to identify its source for intrusion detection.

Hyowon Lee *et al*. [31] have presented a system under development based on users interacting with detected video objects. We outline the suite of technologies needed to achieve such a system and for each we describe where we are in terms of realizing those technologies. We also present a system interface to this system, designed with user needs and user tasks in mind.

Alan J. Lipton *et al*. [32] have outlined two examples indicating that AVS based on computer vision technology is a useful piece of the solution for asset protection, perimeter monitoring, and threat detection. The Logan airport example demonstrates that this technology is desirable over other technologies because it is passive, relatively inexpensive, operationally effective, and provides real-time, actionable intelligence. This technology, however, comes with the caveat that the customer must become educated about its underlying technology and its applicability. Many proponents of computer vision technology are advocating commercial systems that do not perform adequately in real-world environments - they are subject to poor detection rates and high false alarms rates in realistic, unstructured environments. At Objectvideo, we strongly recommend that potential customers trial the technology in their own unique environments to determine the utility of this technology and its adaptability to environmental pressures. Our example shows that the Object video system is, in general, extremely effective as a turnkey system - and in cases with unique environmental phenomena, our system is rapidly adaptable to overcome operational concems.

Sunniva F Meyer *et al*. [33] have explored various trade-offs between standoff and other values, and, when appropriate, proposes possible solutions to such dilemmas. Second, it asks whether employing the SFF in the FGC of Norway will help illuminate these 'troublesome trade-offs'. The analysis has demonstrated that standoff creates challenges for other purposes of the FGC, such as functional office spaces for all employees, but many of these challenges can be solved by planning intelligently, such as creating an external commodity reception. Standoff also creates opportunities for reinforcing social-responsibility requirements, such as accessibility for pedestrians and environmental considerations. The current literature has mostly focused on negative externalities of security, while this paper demonstrates that security measures can have both negative and positive externalities and that planning might alleviate some of the negative ones.

The results, furthermore, support Little's (2004) notion about thinking holistically about protection to create robust and effective security, and show that the academic community can assist in such holistic thinking.

Hae-Min Moon *et al*. [34] have proposed the human identification method that uses height and clothing-color information appropriate for the intelligent video surveillance system based on smartcard. It can obtain reliable feature information using smartcard. In this paper, representative colors are extracted by applying tree-based color quantization technique to the clothing region and height is extracted from the geometrical information of the images. Identification is accomplished by comparing the similarities between two data based on Euclidean distance. From the experiment, we could see that the identification of a human can be checked through the proposed system.

Robin Singh Sidhu *et al*. [35] have proposed information processing techniques for CCTV based surveillance systems employed in (a) work environments and (b) public places and transport, for automated identification of scenes of inter-personal crime. Although both the scenarios presented in this work employ similar signal processing and learning algorithms, the objective involved are significantly different. In (a) we aim to preserve confidentiality and privacy of official meetings and discussions, while ensuring detection of unbecoming behavior, like: bullying, harassment and assault. In the proposed method we identify such critical conditions using a combination of image and speech processing and ensue conditional video recording and saving. In (b), the target is to identify the occurrence of interpersonal crime using video and voice processing, in order to raise alert at the local surveillance station, which may be receiving numerous CCTV videos from neighboring areas. This can be an assistance to the security personnel, responsible to monitor large number of screens. The proposed methods can be useful curbing interpersonal violence, and crime against women, in the form of eve teasing, and harassment.

Analytical surveillance can perform the surveillance tasks much more efficient comparing to operator manual monitoring. This had made it getting increased market's interest in recent years. Commonly, closed circuit television (CCTV) is used for security surveillance. However, CCTVs are purely vision output. These silent videos may not provide complete picture of the happening. Sound detection is incorporate into vision surveillance for enhancement. Sound detection is able to detect abnormal sound although happen at camera blind spots or due to intentional blocking.

Tan Teng Teng *et al*. [36] have proposed to use microcontroller embedded system to enhance current CCTV system. Proposed abnormal sound embedded system is to carry out the sound detection, audio processing and analysis. This study is using only single microphone for sound detection. Audio amplitude and frequency range are targeted feature extracted from Fast Fourier Transform (FFT). Abnormal sound of human screaming and glass breaking were classified using decision tree. From experiment, proposed abnormal sound analytical surveillance system test yield average of 88% accuracy detection. We can consider our work is simple and cost effective for field implementation.

2.4. Video based surveillance system

Shaokang Chen *et al*. [37] have reviewed state-of-the-art face recognition techniques for still images and video sequences. Most of these existing approaches need well-aligned face images and only perform either still image face recognition or video-to video match. They are not suitable for face recognition under surveillance scenarios because of the following reasons: limitation in the number (around ten) of face images extracted from each video due to the large variation in pose and lighting change; no guarantee of the face image alignment resulted from the poor video quality, constraints in the resource for calculation influenced by the real time processing. We then proposed a local facial feature-based framework for still image and video-based face recognition under surveillance conditions. This framework is generic to be capable of still-to-still, still-to-video and video-to video matching in real-time. Evaluation of this approach is done for still image and video based face recognition on LFW image dataset and MOBIO video dataset.

2.5. Video visualization system

Video visualization (VV) is considered to be an essential part of multimedia visual analytics. Many challenges have arisen from the enormous video content of cameras which can be solved with the help of data analytics and hence gaining importance. However, the rapid advancement of digital technologies has resulted in an explosion of video data, which stimulates the needs for creating computer graphics and visualization from videos. Particularly, in the paradigm of smart cities, video surveillance as a widely applied technology can generate huge amount of videos from 24/7 surveillance. Fozia Mehboob *et al*. [38] have proposed a state of the art algorithm has been proposed for 3D conversion from traffic video content to Google Map. Time-stamped glyph-based visualization is used effectively in outdoor surveillance videos and can be used for event-aware detection. This form of traffic visualization can potentially reduce the data complexity, having holistic view from larger collection of videos. The efficacy of the proposed scheme has been shown by acquiring several unprocessed surveillance videos and by testing our algorithm on them

without their pertaining field conditions. Experimental results show that the proposed visualization technique produces promising results and found effective in conveying meaningful information while alleviating the need of searching exhaustively colossal amount of video data.

Huan-Ting Chen *et al*. [39] have developed a robust visualization approach for evaluating the coverage of CCTV systems in public building spaces. Firstly, a method for modeling CCTV systems in virtual building spaces is presented. The emphasis is placed on offering a visual representation of the CCTV coverage in a BIM-based virtual environment. By simulating varifocal lenses and configuring the parameters of Revit cameras, the developed approach simulates the CCTV screen views to provide a better visual demonstration of the working of the CCTV systems. This is advantageous in the checking of design conflicts and effective communication between owners and contractors. The filled regions displayed in the 3D environment are also apparent, allowing accurate visual evaluation of CCTV coverage. Finally, in the case study of an MRT station, the developed approach is shown to be effective and can be widely applied to other building spaces under similar conditions. Table 1 shows the comparison of various methods proposed in the security surveillance system.

Table 1. Comparison of Various Methods Proposed in the Security Surveillance System

Author	Methods	Merits	Demerits
Suzhi Bi *et al.* [42]	Graph-based Cyber Security Analysis of State Estimation in Smart Power Grid.	The graphical characterization of state estimation security provides intuitive visualization of some complex problem structures and enables efficient graphical solution algorithms, which are useful for both defending and attacking the ICT system of the smart grid.	Solving the complex cyber security problems are yet to be considered.
Jianwei & Chen *et al*. [43]	Reconfigurability Based Security Service Path Construction Scheme	The proposed scheme meets the security requirements and greatly improves the efficiency of network resources.	Performance need to be improved in-depth analysis of SAR, determination of network trust values, the scheme scalability over larger scale networks.
Emanuele Ciapessoni *et al.* [44]	Probabilistic Risk-Based Security Assessment of Power Systems Considering Incumbent Threats and Uncertainties	The added value of the proposed approach with respect to conventional security analyses in dealing with uncertainty of threats, vulnerabilities, and system response.	It gives hidden failures, operators' delays and delayed protection, intervention on power system.
Lucas Silva Figueiredo *et al*. [45]	Privacy, Security, and Reliability for Gesture-Based Programming	Gives better programming and reasoning about gesture safety, security, and privacy.	Need improvement for automatically inferring prepose programs by demonstration.
M. Shamim Hossain *et al*. [46]	Toward End-to-End Biomet rics-Based Security for IoT Infrastructure.	Sensors or smartphones capture a face image and securely transmit it to the IoT platform to provide.	Fusing can be done in multimodal non-invasive biometrics in real time to secure IoT industries.
Tian-en Huang *et al.* [47]	Distributed Computing Platform Supporting Power System Security Knowledge Discovery Based on Online Simulation.	Improves computing efficiency and perform better than a centralized platform	Online simulation-based power system security knowledge discovery process shows low performance.
Mahdi Jamei *et al.* [48]	Micro Synchrophasor-Based Intrusion Detection in Automated Distribution Systems.	It's robust, due to its distributed nature; it can be used both to verify existing cyber security systems and to detect potential cyber attacks and it can be inexpensively deployed at existing utilities.	More time complexity.

3. ATTACKS ON VIDEO SURVEILLANCE SYSTEM

3.1. Visual Layer Attacks

a. Stage one : Malicious firmware update over USB port (or) Remotely via a command injection (or) Malicious firmware update over a web interface (or) the VSS or CCTV system could be sold through legitimate sales channel with the malware already pre-installed
b. Stage two: Malicious component is triggered and controlled via a malicious imagery inputs (when such imagery is visualized by the cameras and the video sensors).
c. Hardware based backdoors (attack is implemented in hardware)
d. In order to guarantee both secure and privacy preserving VSS, a strong light weight hybrid cryptosystem (based on multiparty key-sharing scheme) should be deployed in order to prevent privacy and visual layer attacks by malware inside the VSS.

3.2. Covert channel attacks

a. Manipulating LEDs/ IR LEDs from software/firmware (CCTV and VSS usually have plenty of LEDs both on core equipment as well as CCTV cameras installed outside).
b. Attacker could send command and control data to the CCTV cameras via the IRLED;s messaging,
c. Guri *et al*. [40] presented *VisisSploit*, a new type of optical covert channel that leak data through a standard computer LCD display
d. Tainting of video frames (process could detect suspicious code which tries to process the video frames) is a solution in order to detect such attacks.
e. Another solution to detect such attacks could be the use of performance counters

3.3. Steganography attacks

a. Attacker need to capture the digital image snapshots from well-known URLs and recover the infiltrated data.
b. Automatic methods for steganography detection is needed.

3.4. Pan-tilt-zoom attacks

a. PTZ is feature of CCTV cameras that allow them to move in any direction in 3D which is generally controlled by PTZ data protocols.
b. PTZ commands can be sent to PTZ capable cameras from specialized PTZ controls or from software.

3.5. Audio layer attacks

Compromised VSS component can use the audio layer as a command and control channel using hidden voice command techniques [41].

3.6. Denial of service and jamming attack

Uninterrupted and untampered operation is critically important for VSS and producing a DoS attack on CCTV systems even for 1 minute could make them miss an important event.
Table 2 shows the comparison of various attacks and the solution in video surveillance system.

Table 2 Comparison of various security attacks and the solutions in video surveillance system

Name Of Attack Type	Problems caused by this attack	Solutions Developed
Visual Layer Attacks	Costin [49] presented first such an attack on CCTV cameras as the visual layer backdoors. Mowery *et al.* [50] implemented a full body scanner as the secret knock image.	A solution to detect such was developed by J. Newsome *et al.*[51] of video frames. Another method was developed by Castiglione *et al.* [52] using VSS, a cryptographically-strong system could be used similar to the one.
Covert Channels Attacks	Though sometimes the LEDs are physically linked to the hardware and cannot be controlled from software/firmware, recent attacks show that manipulating LEDs from software/firmware becomes increasingly practical and feasible [40]. The attacker could then send command and control data to the CCTV cameras via the IR LEDs messaging (instead of coded visual images). Such a channel would constitute an addition to the classical (W)LAN and Internet channels used for communication and compromise [51].	Guri *et al.* [40] presented VisiSploit, a new type of optical covert channel that exploits the limitations of human visual perception in order to unobtrusively leak data through a standard computer LCD display.
Denial-of-Service and Jamming Attacks	Producing a DoS attack on a CCTV systems even for 1 minute could make them miss an important event such as an extremely fast bank robbery [53].	DoS attacks on video surveillance systems have critical impact and have to be taken into consideration during design, evaluation and testing [53].

4. DESIGN GOALS ON VIDEO SURVEILLANCE SYSTEM

4.1. Design requirements

a. Should be secure but low cost in implementation
b. Should provide end-to-end system security throughout the entire distribution chain

c. Should sustain current and new heterogeneous environment to attract more applications and more customers
d. Should be scalable from distributed caches and storage device to heterogeneous client devices
e. Should be extendable from PCs to mobile devices and still remain secure, for flexible new business models
f. Should be easily renewable
g. Should not reduce the playback quality of the streaming media, i.e., it should not impact continuous playback, loss resilient capability, and scalability of the system in real time streaming applications
h. Should be able to preserve entertainment like experience – users should be able to fast-forward or rewind content without any degradation on the viewing or playback experience

4.2. Design should focus on

a. Factory reset button-to reset the system to a known factory safe and secure image and state from non-volatile , non-writable secure memory chip
b. Secure scan chains-Implementing secure scan techniques which allows secure debugging, testing, restoring without the risk of unauthorized users to gain access and debug.
c. Remote Software-Implementing remote software technique to ensure the security is not tampered.
d. Formal proof and verification-Applying some formal proof in order to ensure the hardware design, firmware implementation, communication and security protocols.
e. Standard compliance-Implementing software and hardware security compliance standards.
f. Artificial Intelligence-Implementing image-tracking facility which must have the features for identifying tail-gating, vehicle detection features, unattended baggage identification, queuing analysis, and external text insertion feature and intruder detection.
g. Privacy-Implementing ways that protect the privacy of the individuals including privacy enhancing technologies.

5. CONCLUSION

Detecting the persons and analyzing their behavior by means of visualization is a prime factor for the computer systems nowadays to interact cleverly in a few human populated areas. Visual surveillance systems are used for the real time surveillance of targets like persons or vehicles will lead to the description of objects' activities in that environment. Visual surveillance has been used for security observation, anomaly recognition, and interloper detection, computing traffic flow, mishap detection on the highways and scheduled maintenance. We have provided a detail survey on video surveillance system, attacks and their design goals for implementing CCTV video surveillance system. Therefore, there is need of efficient CCTV surveillance with higher performance rate and less computation cost. We hope the discussion made in this paper will provide a valuable knowledge as well as promote further research and widen the scope of this field beyond its current boundaries.

ACKNOWLEDGEMENTS

This work was supported by the Korean Federation of Science and Technology Societies (KOFST) grant funded by the Korean government (MSIP: Ministry of Science, ICT and Future Planning).

REFERENCES

[1] H. M. Dee and S. A. Velastin, "How close are we to solving the problem of automated visual surveillance: A review of real-world surveillance, scientific progress and evaluative mechanisms", *Machine Vision and Applications*, 2007.
[2] A. Hampapur, L. Brown, J. Connell, A. Ekin, N. Haas, M. Lu, H. Merkl, S. Pankanti, A. Senior, C.-F. Shu, and Y. L. Tian, "Smart video surveillance: Exploring the concept of multiscale spatiotemporal tracking", *IEEE Signal Processing Magazine*, pp. 38-51, March 2005.
[3] Brovko, N., and R. Bogush, "Smoke detection algorithm for intelligent video surveillance systems", *Computer Science Journal of Moldova*, vol. 21, no. 1(61), 2013.
[4] S. Amarnag, R. S. Kumaran, and J. N. Gowdy, "Real time eye tracking for human computer interfaces", in *IEEE International Conference on Multimedia and Expo*, Washington, DC, USA, pp. 557-560, 2003
[5] H. M. Dee and S. A. Velastin, "How close are we to solving the problem of automated visual surveillance: A review of real-world surveillance, scientific progress and evaluative mechanisms", *Machine Vision and Applications*, 2007.
[6] B. Aldred, "London Underground Platfrom to Train CCTV Studies", *IEEE WC2R*, Savoy Place, London, UK, pp. 1-12, 2000.
[7] D. Ferraiolo, J. Barkley, and D. Kuhn, "A Role-Based Access Control Model and Reference Implementation within

a Corporate Intranet", *ACM Transactions on Information and System Security*, vol. 2, Feb. 2000.
[8] C. Busch, W. Funk, and S. Wolthusen, "Digital Watermarking: from Concepts to Real-Time Video Applications", *IEEE Computer Graphics and Applications*, vol. 19, pp. 25-35, Jan 1999.
[9] Senior, Andrew, Sharath Pankanti, Arun Hampapur, Lisa Brown, Ying-Li Tian, Ahmet Ekin, Jonathan Connell, Chiao Fe Shu, and Max Lu, "Enabling video privacy through computer vision", IEEE Security & Privacy, vol. 3, no. 3, pp 50-57, 2005.
[10] "Selection of Cameras, Digital Recording Systems, Digital High-Speed Networks and Train lines for Use in Transit-Related CCTV Systems", *American Public Transportation Association, IT-CCTV-RP-001-11* June 2011.
[11] A. Chattopadhyay and T. Boult, "PrivacyCam: A Privacy Preserving Camera Using uCLinux on the Blackfin DSP", *IEEE Conf. on Computer Vision and Pattern Recognition*, pp. 1-8, Jun. 2007.
[12] P. Tuyls, E. Verbitskiy, J. Goseling, and D. Denteneer, "Privacy protecting biometric authentication systems: an overview", *European Signal Processing Conference*, pp. 1397-1400, 2004.
[13] Sagar Badgujar, Amol Mahalpure, Priyaka Satam, Dipalee Thakar, Swati jaiswal, "Real time number plate recognition and tracking vehicle system", *SSRG International Journal of Computer Science and Engineering*, vol. 2, no. 12 December 2015.
[14] Li, Bin, Jian Zhang, Zheng Zhang, and Yong Xu, "A people counting method based on head detection and tracking", *IEEE International Conference in Smart Computing*, pp. 136-141, 2014.
[15] A. Cavallaro, "Privacy in video surveillance IEEE Signal Process", *Magazine*, vol. 24, no. 2, pp. 166-168, Mar, 2007.
[16] Dong-Ik Ko, G. Agarwal, "Gesture recognition: Enabling natural interactions with electronics", *Texas Instruments white paper*, SPRY199, 2012.
[17] Lin, Kuan Jen, Tsai Kun Hou, and Rui Jen Chiu, "Jitter-constrained camera scheduling in CCTV surveillance networks", *IEEE International Conference on Signal and Image Processing*, pp. 650-654, 2016.
[18] Li, Liyuan, Weimin Huang, Irene Yu-Hua Gu, Ruijiang Luo, and Qi Tian. "An efficient sequential approach to tracking multiple objects through crowds for real-time intelligent CCTV systems", *IEEE Transactions on Systems, Man, and Cybernetics, Part B*, vol. 38, no.5, pp. 1254-1269, 2008
[19] Ming, Y., J. Jiang, and F. Bian, "3D-City Model supporting for CCTV monitoring system", *International Archives of Photogrammetry Remote Sensing and Spatial Information Sciences*, vol. 34, no. 4, pp 456-459, 2002
[20] Atrey, Pradeep K., M. Anwar Hossain, and Abdulmotaleb El Saddik, "Automatic scheduling of CCTV camera views using a human-centric approac", *IEEE International Conference on Multimedia and Expo*, pp. 325-328, 2008.
[21] Coleman, Roy, and Joe Sim, "You'll never walk alone: CCTV surveillance, order and neo- liberal rule in Liverpool city centre1", *The British journal of sociology*, vol. 51, no. 4, pp. 623-639, 2000.
[22] Tae Hyung, Kim, "Next generation architecture examination for Mass Notification System (MNS) collaborating with CCTV for Smart & Safe City", *International Journal of engineering Research and Applications*, vol. 5, no. 3, pp. 39-45, March 2015.
[23] Han, Byoung-Jin, Hyuncheol Jeong, and Yoo-Jae Won, "The privacy protection framework for biometric information in network based cctv environment", *IEEE Conference on Open Systems*, pp. 86-90, 2011.
[24] Saponara, Sergio, Luca Pilato, and Luca Fanucci, "Exploiting CCTV camera system for advanced passenger services on-board trains", *IEEE International in Smart Cities Conference*, pp. 1-6, 2016.
[25] Nguyen, Hoang Thanh, Bir Bhanu, Ankit Patel, and Ramiro Diaz, "Design and optimization of the videoweb wireless camera network", *EURASIP Journal on Image and Video Processing*, no. 1, 865803, 2010
[26] Bhavani, anabham, Tulasi jami, And Gajjala ashok, "Low Cost Smart Security Camera with Night Vision Capability Using Raspberry Pi and PIR Sensor", *Int. Journal of advanced technology and innovative research*, vol 8, no. 21, pp. 4053-4056, 2016.
[27] Hargude, Sonali, and S. R. Idate, "I-surveillance: Intelligent surveillance system using background subtraction technique", *International Conference in Computing Communication Control and automation*, pp. 1-5, 2016.
[28] Havârneanu, Grigore M., Marie-Hélène Bonneau, and Jacques Colliard, "Lessons learned from the collaborative European project RESTRAIL: REduction of suicides and trespasses on RAILway property", *European Transport Research Review*, vol. 8, no. 2, pp. 1-15, 2016.
[29] Jyothi, S. Naga, and K. Vijaya Vardhan, "Design and implementation of real time security surveillance system using IoT", *International Conference in Communication and Electronics Systems*, pp. 1-5, 2016.
[30] Lapeña, Patricia Marie L., Joseph Ian Q. Blanco, Kevin I. Bunda, Arnold Gabriel S. Cruz, Aaron I. Ramirez, and Argel A. Bandala, "Swarm algorithm implementation in mobile robots for security and surveillance", *IEEE Region 10 Conference in TENCON 2014-2014*, pp. 1-5, 2014.
[31] Lee, Hyowon, Alan F. Smeaton, Noel O'Connor, and Noel Murphy, "User-interface to a CCTV video search system", *The IEEE International Symposiumc in Imaging for Crime Detection and Prevention*, pp. 39-43, 2005.
[32] Lipton, Alan J., Craie H. Heartwell, Niels Haering, and Donald Madden, "Automated video protection, monitoring & detection", *IEEE Aerospace and Electronic Systems Magazine*, vol. 18, no. 5, pp 3-18, 2003
[33] Meyer, Sunniva F., Sissel H. Jore, and Kjell W. Johansen, "Troublesome trade-offs: balancing urban activities and values when securing a city-centre governmental quarter", *City, territory and architecture*, vol. 2, no. 1, 2015.
[34] Moon, Hae-Min, and Sung Bum Pan, "A new human identification method for intelligent video surveillance system", *Proceedings of 19th International Conference on Computer Communications and Networks*, 2010.
[35] Sidhu, Robin Singh, and Mrigank Sharad, "Smart surveillance system for detecting interpersonal crime", *IEEE International Conference on Communication and Signal Processing*, pp. 2003-2007, 2016.
[36] Teng, Tan Teng, Lim Tien Sze, and Ong Lee Yeng, "Abnormal sound analytical surveillance system using

microcontroller", *IEEE 12th International Colloquium in Signal Processing & its Applications*, pp. 162-166, 2016.
[37] Chen, Shaokang, Sandra Mau, Mehrtash T. Harandi, Conrad Sanderson, Abbas Bigdeli, and Brian C. Lovell, "Face recognition from still images to video sequences: a local-feature-based framework", *EURASIP journal on image and video processing*, no. 1, 790598, 2011.
[38] Mehboob, Fozia, Muhammad Abbas, Saad Rehman, Shoab A. Khan, Richard Jiang, and Ahmed Bouridane, "Glyph-based video visualization on Google Map for surveillance in smart cities", *EURASIP Journal on Image and Video Processing*, no. 1, pp. 28, 2017.
[39] Chen, Huan-Ting, Si-Wei Wu, and Shang-Hsien Hsieh, "Visualization of CCTV coverage in public building space using BIM technology", *Visualization in Engineering*, vol. 1, no. 1, pp. 5, 2013.
[40] M. Guri, O. Hasson, G. Kedma, and Y. Elovici, "Visisploit: An optical covert-channel", *arXiv preprint arXiv*:1607.03946, 2016.
[41] N. Carlini, P. Mishra, T. Vaidya, Y. Zhang, M. Sherr, C. Shields, D. Wagner, and W. Zhou, "Hidden Voice Commands", *In 25th USENIX Security Symposium* , Austin, TX, 2016.
[42] Bi, Suzhi, and Ying Jun Angela Zhang, "Graph-based Cyber Security Analysis of State Estimation in Smart Power Grid", *IEEE Communications Magazine*, 2017.
[43] Chen, Jie, Jianwei Liu, Kefei Mao, Mengmeng Wang, and Haosu Cheng, "A Reconfigurability Based Security Service Path Construction Scheme", *IEEE Access*, 2017.
[44] Ciapessoni, Emanuele, Diego Cirio, Gerd Kjølle, Stefano Massucco, Andrea Pitto, and Marino Sforna, "Probabilistic Risk-Based Security Assessment of Power Systems Considering Incumbent Threats and Uncertainties", *IEEE Transactions on Smart Grid*, vol. 7, no. 6, pp 2890-2903, 2016.
[45] Figueiredo, Lucas Silva, Benjamin Livshits, David Molnar, and Margus Veanes, "Prepose: Privacy, Security, and Reliability for Gesture-Based Programming", *IEEE Symposium in Security and Privacy*, pp. 122-137, 2016.
[46] Hossain, M. Shamim, Ghulam Muhammad, Sk Md Mizanur Rahman, Wadood Abdul, Abdulhameed Alelaiwi, and Atif Alamri, "Toward end-to-end biomet rics-based security for IoT infrastructure", *IEEE Wireless Communications*, vol. 23, no. 5, pp. 44-51, 2016.
[47] Huang, Tian-en, Qinglai Guo, and Hongbin Sun, "A Distributed Computing Platform Supporting Power System Security Knowledge Discovery Based on Online Simulation", *IEEE Transactions on Smart Grid*, 2016.
[48] Jamei, Mahdi, Emma Stewart, Sean Peisert, Anna Scaglione, Chuck McParland, Ciaran Roberts, and Alex McEachern, "Micro synchrophasor-based intrusion detection in automated distribution systems: Towards critical infrastructure security", *IEEE Internet Computing*, vol. 20, no. 5, 2016.
[49] A. Costin. "Poor Man's Panopticon: Mass CCTV Surveillance for the masses", *In Power of Community*, November 2013.
[50] K. Mowery, E. Wustrow, T. Wypych, C. Singleton, C. Comfort, E. Rescorla, J. A. Halderman, H. Shacham, and S. Checkoway, "Security analysis of a full-body scanner", *In 23rd USENIX Security Symposium* , pp 369-384, 2014.
[51] J. Newsome and D. Song, "Dynamic taint analysis for automatic detection, analysis, and signature generation of exploits on commodity software", 2005.
[52] A. Castiglione, M. Cepparulo, A. De Santis, and F. Palmieri, "Towards a lawfully secure and privacy preserving video surveillance system", *In International Conference on Electronic Commerce and Web Technologies*, pp. 73-84. Springer, 2010.
[53] M. Brocker and S. Checkoway, "iSeeYou: Disabling the MacBook webcam indicator LED", *In 23rd USENIX Security Symposium*, pp. 337-352, 2014.
[54] J. Aron. Want to rob a bank? Hack your way in. New Scientist, 220(2937):22, 2013.

BIOGRAPHIES OF AUTHORS

Balasubramanian Muthusenthil received the degree in Electronics & Communication Engineering from Madras University, in 1996 Master's Degree from Satyabama University in 2007, Doctorate from Anna University, Chennai 2016. Currently, he is a Research Scientist in Wookyoung Information technology, Daegu, Southkorea and Associate Professor at Valliammai Engineering College, Chennai. His interests are in mobile ad-hoc networks, network security, video security, network attacks, privacy preservation, trust evaluation and cloud computing.

Hyunsung Kim received his MSc. and Ph.D. degrees in Computer Engineering from Kyungpook National University, Republic of Korea, in 1998 and 2002, respectively. From 2000 to 2002, he worked as a senior researcher at Ditto Technology. He had been an associate professor from 2002 to 2011 with the Department of Computer Engineering, Kyungil University. Currently, he is a professor at the Department of Cyber Security, Kyungil University.His current research interests are cryptography, VLSI, security protocols, network security and ubiquitous computing security