ISSN NO. 2320-5407

Journal homepage: http://www.journalijar.com

INTERNATIONAL JOURNAL OF ADVANCED RESEARCH

RESEARCH ARTICLE

Various surveillance techniques, a concise review

***Ruchira Susar, and Prof.M.P.Dongare**
Department of Electronics, Amrutvahini college of engineering,Sangamner,India

Manuscript Info

Manuscript History:

Received: 14 November 2015
Final Accepted: 15 December 2015
Published Online: January 2016

Key words:

Surveillance,
CCTV, Biometrics, Body scanners,
Unmaned aerial vehicles

Corresponding Author

Ruchira Susar

Abstract

It is very important to encompasses the identification and description of current and emerging surveillance technologies for improvement. Different techniques of surveillance are evaluated with regard to their potential to providing real opportunities in practise. So the outcome of this analysis is not to be seen as a stand-alone, but will serve as input for the other sub-tasks to choose appropriate technology to accomplish your purpose.

To provide a well-researched basis for such an assessment, a number of surveillance technologies are selected to describe their functionality and effectiveness from a technological point of view. Since a description of the full range of all existent surveillance technologies is not possible within the scope, here tried to select technologies which have a great impact on the lives of citizens nowadays and will continue to have a great impact in the nearby future.

INTRODUCTION

One can define surveillance as the targeted or systematic monitoring by governmental organizations and their partners, of persons, places, items, infrastructures or flows of information, in order to identify hazards and manage risk and to enable, typically, a preventive, protective or reactive response, or the collection of data for preparing such a response in the future. Hence one can say that, the major aim of surveillance is to name, identify, monitor and track individuals and their actions. Following is given brief explanation of different techniques of surveillance which are existing and also emerging [1].

Classification:

To empower the reader in terms of easier orientation, the selected technologies are classified into four sections, which are:

- Public space surveillance
- Network & targeted device surveillance
- Biometrics & body scanners
- Data matching, linkage & analysis

Brief taxonomy of surveillance technologies can be seen in fig 1.

Public space surveillance

The surveillance of public places is mostly perceived by citizens as being monitored while situated in spaces open to the public, and thus comes with a Janus face. On the one hand, surveillance is seen as a measure of prevention and protection against security threats likely to happen in public spaces such as public squares and buildings, streets, parks and other publicly accessible areas of the country [2,9]. Here technologies described are dedicated to public space surveillance with a focus on the two most relevant approaches: CCTV and drones.

Drones

Drones are generally referred to as Unmanned Aerial Vehicles (UAV) or Unmanned Aerial Systems (UAS). In fact, more than 1,000 UAV systems exist today worldwide. Drones are, like Smart CCTV, a technical approach to conducting the surveillance of public spaces for the purpose of enhancing security. They represent the latest domestic application of a technology first employed in the military field during World War I; the first earnest deployment of an unmanned aerial vehicle was Archibald Montgomery Low's 'Aerial Target' in 1916. However, drones gained greater public attention when an armed drone became known to have been involved in the targeted killing of high-ranking Al-Qaeda military commander Mohammed Atef in Afghanistan in November 2001[9]. Since then, the U.S. have used unarmed as well as armed drones in a number of foreign countries beyond Afghanistan (e. g. in Pakistan, Yemen, Somalia and Iraq) and also in the domestic area in different contexts and for different reasons. More than 70 other countries worldwide have followed this example and now use this new technology for a variety of purposes [9].

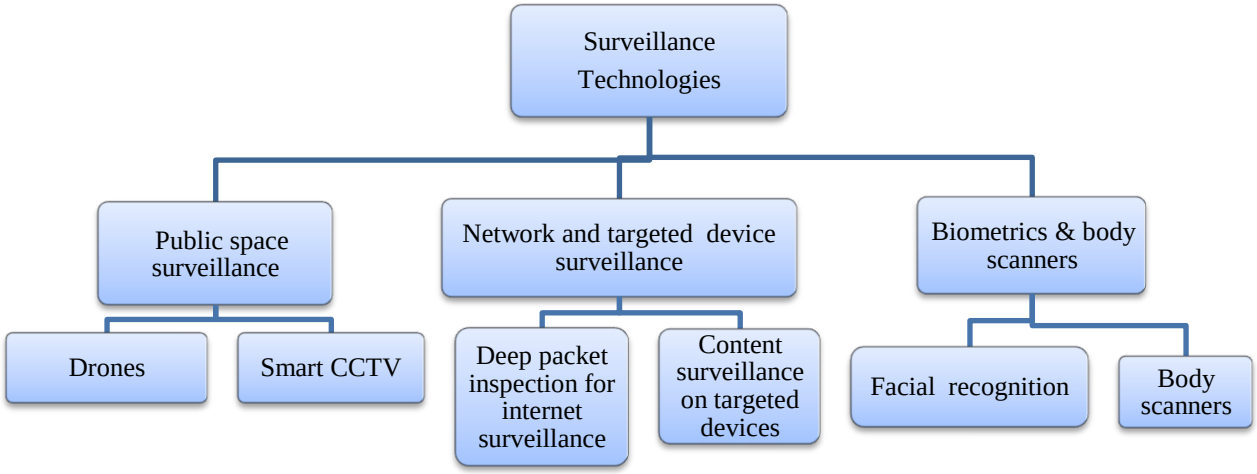

Fig. 1 Taxonomy of surveillance technologies

Smart CCTV

In Smart CCTV (Closed Circuit Television), a significantly more comprehensive surveillance of citizens in public space areas is conducted, involving advanced features of the technology such as face & motion detection, crowd & directional flow detection, unattended or missing object detection, facial recognition, license plate recognition, targeting/positioning/tracking of subjects and objects, behavioural pattern & anomaly recognition, image quality & camera zooming enhancement, audio recording, and additional data matching & analytics capabilities.

In the wake of the terrorist events in September 2001, a multitude of surveillance technologies have been increasingly used for security purposes. Closed Circuit Television (CCTV) has been one of them [4]. And indeed, the deployment of CCTV technologies in numerous countries, including European Union member states, has been increasing ever since and continues to grow. However, while at first the terrorist attacks of 2001 triggered a worldwide political and societal desideratum to counter similar future dangers with the help of video surveillance, CCTV is becoming more and more common as a tool not only for simpler local crime prevention, but also for investigating minor offences. Ideally, the national law of the respective countries foresees certain preconditions for the usage of public space visual observation, such as the fulfilment of a specific legal ground, the requirement of necessity, a legitimate purpose and the proportionality between the privacy impacts on citizens vs. the effectiveness of the measure to achieve the intended purpose.

Network and targeted device surveillance

This section focuses on surveillance-oriented security technologies related to the monitoring of live traffic and data being transmitted through networks as well as on the surveillance of specific static or mobile devices of

individuals. Several methods to monitor and filter networks exist, for example HTTP proxy filtering, combined (hybrid) TCP/IP and HTTP proxy filtering, DNS tampering, distributed denial of service (DDOS) attacks, and also Internet domain registration and server take downs**.**

Deep Packet Inspection for Internet surveillance

Deep Packet Inspection (DPI) is a technology which can be used to extract user data which is sent between different devices via networks. Depending on the concrete design and deployment of the DPI technology, it is possible to perform the surveillance measure on a broad scope via the respective

Internet Service Provider (ISP). Internet surveillance means the monitoring of data and traffic on the Internet. As the Internet is arguably the most important communication channel, governments globally perceive this medium as a danger to security as well as a chance to obtain information useful in preventing and investigating security threats and incidents. Looking for direct access to information, governmental agencies worldwide turn mainly to the providers of broadband Internet connection and Voice-over-Internet-Protocol (VoIP) services. Seeking to oblige these providers to employ their own infrastructure capacities to constantly monitor, screen, analyse and filter data traffic, high hopes are set on this approach to identify terrorists and other criminals.

Here presented forms of Internet surveillance as a broad concept to monitor or screen communication routed through a network node. Social media providers such as Google, Facebook etc. may have the ability to implement DPI into their own systems to surveil the content uploaded to their servers and give access to security agencies which leads to solve most of criminal cases.[3,9]

The core technology to achieve the surveillance of the means of communication between citizens is the deployment of Deep Packet Inspection technology, allowing for an extensive monitoring and analysis of data packets being sent via the Internet. Internet service providers can deploy DPI within their own infrastructures to scan the traffic being routed via their servers, e. g. to achieve:

- Network stability
- Network/Bandwidth management
- Content filtering, spam detection, and blocking of websites
- Rerouting e. g. to own search sites in case a website is not directly accessible
- Profiling for targeted advertising
- Manipulation of websites for more efficient transmission
- Provision of governmental surveillance and censoring infrastructures
- Blocking of encryption and tunnelling systems preventing lawful interception

Content surveillance on targeted devices

From the viewpoint of security agencies, the surveillance of citizens telecommunication is a key tool to enable effective crime prevention as well as crime investigation. The conventional methods of telecommunication surveillance enable the direct extraction of data during a running telecommunication process. However, during Internet-based telecommunication, these methods are often not sufficient for their usual purpose. This is owing to the fact that typically the telecommunication providers are not able to ensure the extraction of unencrypted data, whereas deciphering encrypted data is usually difficult at best. Consequently, telecommunication surveillance can be achieved by collecting and deriving the data directly from the device of the targeted individual before the encryption process occurs, or, alternatively, when it gets unencrypted. In these cases, technology for network communication and data packet inspection are brought onto the individual devices by means of Trojan Horses, and thereby creating a backdoor to the system. This opens up the possibility of effective communication interception. Also, beyond the mere interception of telecommunication, it possibly enables further means of surveillance, for example by being accompanied by additional malware. These may go far beyond mere wiretapping of Internet telephony up to complete online searches of targeted devices [5].

How it works:

The infiltration of a specifically targeted device in contrast to wide-range Internet surveillance occurs through software which was brought onto the personal system. This software, most often a Trojan Horse, functions covertly, without revealing its real functionalities to the user of the device. In fact, it may also be complemented by DPI technology as a remote tool to capture the telecommunication data before it gets encrypted to leave the device on its transmission route. Then the network capabilities of the specific device are used to transmit its obtained data as a sending entity to a receiving entity, where it is directly accessible for the executing governmental agencies. This receiving entity in turn sends commands to the sending entity to initiate or control specific operational functionalities (see Figure 2). The exchange between both entities usually occurs over one or several proxy servers to disguise the route of the connection [7].

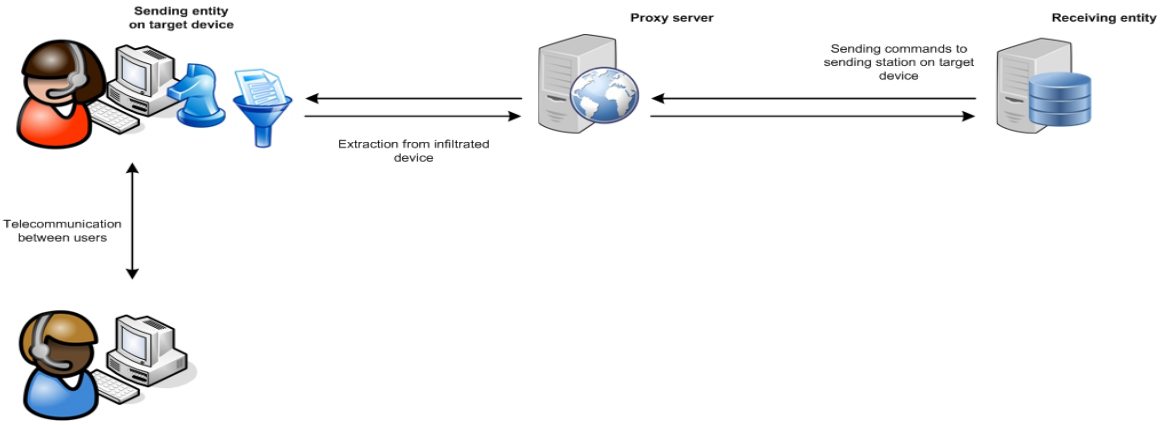

Fig. 2 Extraction of data from infiltrated device

Location tracking

The modern days of mobile communication have led to a significant expansion of technologies providing a variety of location systems. These serve a multitude of different purposes in several areas, ranging from military, health care, retail and postal. The mobility of persons and assets has thus become another aspect of security in public space, thus reinforcing the desire of intelligence and police agencies to obtain geo location information where needed. In an attempt to define the difference between location and geo location, it can be said that location is a more vague term relating to a certain attribute, such as a city district or street name; geo location, however, is represented by very precise geographic position information by means of latitude, longitude and altitude coordinates. In this context, most real-time location systems nowadays are built-in wireless systems [8]. Most of these technologies entail a so-called location-based system which consists of five basic components needed for the functionality of the service. These components are:

- Software application of the service provider
- A mobile network to transmit data and requests for the service
- Content provider supplying the geo-specific information
- A positioning component (GPS)
- End-user's mobile device

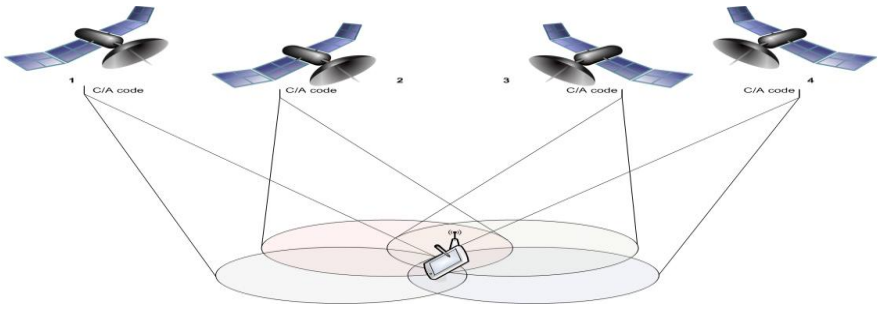

Fig. 3 GPS receiving satellite signals to determine exact time and geolocation

Biometrics & body scanners

Biometric recognition systems and body scanners are two fields of technology being closely tied to the bodily integrity of the concerned target individual. The international Association for Identification defined biometrics as referring to the measurement and analysis of attributes of living things'. The International Organization for Standardization (ISO) developed a series of biometric data format standards known as ISO/IEC IS 19794. The ISO/IEC JTC SC37 Harmonized Biometric Vocabulary (HBV) understands biometrics as "biological and behavioural characteristics of an individual from which distinguishing, repeatable biometric features can be extracted for the purpose of biometric recognition." Thereby, biometric recognition encompasses both biometric verification as well as biometric identification. However, the goal of most biometric recognition systems is either the

identification of an individual, or the verification/falsification of a claimed identity [6]. Though not a conclusive list, examples of such measurable biological and behavioural characteristics are:

- Face topography & facial expression
- Skin texture & colour
- Hand & finger topography
- Ridge structure of hand palm
- Iris structure & retinal pattern
- Vein structures
- Signature pattern & dynamics
- Voice acoustic patterns

All of such or similar information obtained by biometric measurement methods may under circumstances be subjected to access by security agencies for purposes of crime prevention and crime investigation. This is also due to the fact that biometric characteristics are typically bound to an individual, whereas other identification or authentication systems, such as code, secret password, or the possession of another physical identifier, may be just temporary. Regarding these characteristics, a distinction must be made between so-called static and dynamic characteristics. Static characteristics do not or sparsely change over the lifetime of the individual, such as fingerprints, genetic information etc. Dynamic characteristics are behavioural traits of an individual, such as written signature, facial expression, movement and voice patterns etc.

Facial recognition

Humans predominantly use face recognition to verify the identity of an individual or to perform an identification process. Facial recognition is also one of the biometric techniques being used for this purpose. Since the face of a person is usually visible (unless the person wears a veil, a hood, a helmet or a mask), this biometric method works without cooperation of the person concerned, e. g. When analysing a photo or a video, no matter whether the visual image is taken from a CCTV system or a social network. Already deployed in a number of European and other countries for the enrolment of electronic IDs, it can be used to enable physical or virtual access restriction. Scientists and developers envision further applications for facial recognition, e. g. in e-commerce in combination with the use of Smart Cards e. g. for online banking, and in covert surveillance conducted by governmental security agencies [6]. Within potential civil use, facial recognition as part of a wider spectrum of biometrics is interesting to companies owing to a number of reasons. So key explanations of its widespread adoption not only include its prevention of unauthorised access and fraud, but also its enhancement of administrative efficiency. Entities that use facial recognition systems may see potential benefits in a great variety of areas, for example:

- Administration costs
- Identification & information integrity
- Physical and virtual access control
- Delivery speed regarding services and benefits
- Research and statistics accuracy and quality

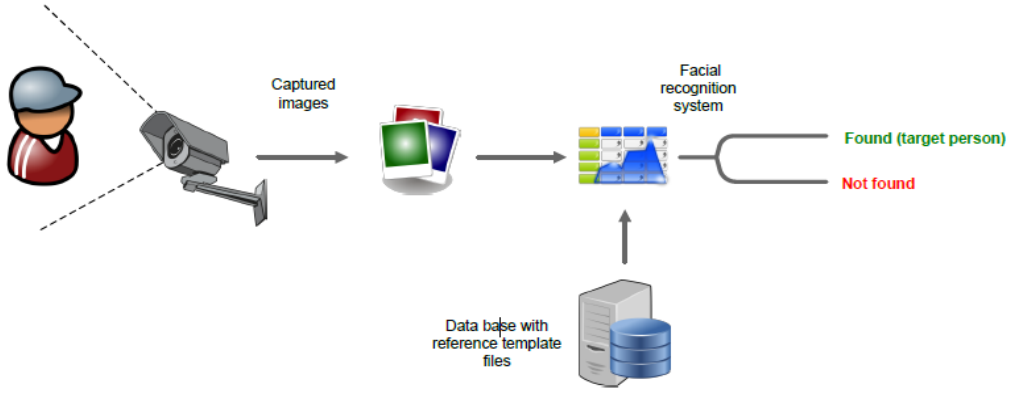

Fig. 4: Facial recognition process, checking against a data base of target persons

Body scanners

A full-body scanner is a device used to detect in a visual way any (forbidden) object which people may have (hidden) in their clothing or even (with X-rays) in their bodies. One difference between full-body scanners and conventional metal detectors is that this technology displays an image of the scanned individual without the clothing, in various levels of detail, depending on the device used. Due to that fact, some scanner types are considered very invasive with regard to privacy. Also, some scanner types may produce adverse health effects.

Actually body scanners are not by definition a technology directly related to biometrics. However, they also concern bodily data and bodily integrity of individuals. The constant conflict between privacy and security is often at the core of public discussion, focusing on the fact that after the terrorist attacks of 9/11, Madrid and London, governments have increasingly deployed a variety of security measures. One of these measures is body scanners, a fairly new technology believed by experts able to guarantee security in a more efficient way than traditional methods are able to secure, e. g. aviation. This is believed to be so owing to the fact that the new-generation body scanners would be able to accurately detect liquids and non-metallic objects. But the introduction of these new scanner technologies is also heavily criticized for serious implications regarding data protection and privacy as well as regarding other fundamental rights of citizens. Now a day's these technologies are being implemented at a number of airports, with the U.S. perceived as the most intensely deploying nation, but some countries following the example [7,9]. This occurs partly with an already fixed establishment of body scanners and partly just with first tentative test runs. Already, security agencies consider the use of body scanner technologies helpful in securing not only airports, but also the entrances of public buildings, bus and train stations.

Four different types of body scanners technologies:

- Millimetre waves

The image is generated by the natural radiation of millimetre waves emitted by the body or reflected by what surrounds it. The main advantage of this technology is the absence of radiation. The main disadvantage lies in the fact that the body images are very elementary and fuzzy. However, hidden objects (metallic and non-metallic) are shown.

- Active millimetre waves

The body is illuminated by means of reflected short-wave radio waves to generate the image. This technology works on frequencies between approximately 30 and 300 GHz. This system has two advantages: the images created are high resolution so any object will be seen, and the surface of the body is shown in detail.

- X-ray backscatter

The backscattered radiation illuminates the body with low-dose X-rays to create a two dimensional image of the body.

- X-ray transmission imagery

This technology also uses X-rays to produce images. In contrast to the aforementioned technique, these rays penetrate the clothing and body similar to the X-rays used in medicine for detecting metallic or non-metallic objects which have been swallowed or introduced into body cavities.

Conclusion

Here described the vast possibilities Smart CCTV and drones provide for observing public space areas, and we introduced to some very effective means of surveillance in the digital sphere. Moreover, surveillance technologies closely tied to the bodily integrity of individuals such as facial recognition and body scanners are also regarded as possible solutions by security agencies. Together with fairly new possibilities of making use of the data collected, for example by certain techniques in the context of Big Data, these technologies provide for ample opportunity to comprehensively scrutinise an individual's personal habits, beliefs, and life conditions. Finding even more solutions to the forementioned issues will in the next few years become a big prospect for new research and development initiatives. It is yet to be seen how they will succeed in reining in groundless excessive data collections and still preserve the chances for providing security to citizens.

Acknowledgment

I would like to express my true sense and a sincerest gratitude to my guide Prof. M.P.Dongare for his dynamic and valuable guidance. I am grateful to him for constant encouragement in the fulfilment of this paper. This work is a result of combined efforts put in by my guide and me. I would also like to thank him for providing me with all necessary infrastructure and facilities to complete the paper.

References

1. Federal Communications Commission News Media Information letter (2005), titled FCC Requires Certain Broadband and VoIP Providers to Accommodate Wiretaps", Foundation (EFF), Legal Struggles Over Interception Rules in the United States.
2. Noah Shachtman and David Axe for Wired.com,(2012,) Most U.S. Drones Openly Broadcast Secret Video Feed
3. Robert Booth in The Guardian(2012) Government plans increased email and social network surveillance.
4. Paul Sonne and Margaret Coker, (2011) The Wall Street Journal Online, "Firms aided Libyan spies – First Look Inside Security Unit Shows How Citizens Were Tracked."
5. The investigation report of the Bavarian Data Protection Commissioner(July 30th 2012,) "Prüfbericht Quellen- pp. 17
6. Cf. Margaret Rouse on Search mobile Computing, definition entry for the term Geolocation
7. International Association for Identification (IAI), website information under Biometrics Information Systems
8. Cf. Walter Kropatsch, Robert Sablatnig, Pattern Recognition and Image Processing Group at the Institute of Computer-aided Automation, Computer Science Department of the Vienna University of Technology, Biometrics
9. Project surprise(2012.2013)Surveillance, Privacy and Security: A large scale participatory assessment of criteria and factors determining acceptability and acceptance of security technologies in Europe