Chapter 16
Visual Sensor Network Processing and Preventative Steganalysis

Julien Sebastien Jainsky
Texas A&M University, USA

Deepa Kundur
Texas A&M University, USA

ABSTRACT

In this chapter, we discuss the topic of security in wireless visual sensor networks. In particular, attention is brought to steganographic security and how it can be discouraged without challenging the primary objectives of the network. We motivate the development and implementation of more lightweight steganalytic solutions that take into account the resources made available by the network's deployment and its application in order to minimize the steganalysis impact on the WVSN workload. The concept of preventative steganalysis is also introduced in this chapter as a means to protect the network from the moment it is deployed. Preventative steganalysis aims at discouraging any potential steganographic attacks by processing the WVSN collected data such that the possibility of steganography becomes very small and the steganalysis leads to high rate of success.

INTRODUCTION

Wireless visual sensor networks (WVSNs) provide unprecedented opportunities to improve surveillance and assisted-living applications. Such broadband and often mobile networks when combined with visual data acquisition provide keen insights for tactical battlefield scenarios, geriatric patient monitoring amongst other applications. This inherent application space makes issues of security and privacy a significant concern while their often aggressive design (maximizing both efficiency and visual utility) makes engineering of security and privacy challenging.

DOI: 10.4018/978-1-61350-153-5.ch016

From a technological perspective, security and privacy may be addressed through an effective marriage between signal processing, communications and applied cryptography. It is imperative that such solutions be studied during system specification and creation rather than applied as an afterthought, which can lead to superficial protection requiring repeated upgrade. In this chapter, we propose to introduce and study the novel yet important problem in WVSN security of *preventative steganalysis*.

BACKGROUND

Most well known measures to protect WVSNs, to date, have focused on the problem of providing privacy in vision-rich systems. Lo *et al.* (Lo, Wang & Yang, 2005) introduce an automated homecare monitoring system for the elderly named *UbiSense* where image processing is conducted directly at the camera to convert visual data directly into abstractions that reveal no personal information and hence protect the privacy of the monitored individuals. Fidaleo *et al.* (Fidaleo, Nguyen & Trivedi, 2004) introduce the *Networked Sensor Tapestry (NeST)* architecture designed for the secure sharing, capture, and distributed processing and archiving of multimedia data. They introduce the notion of "subjective privacy" in which processing of raw sensor data is conducted to remove personally identifiable information; thus the behavior, but not the identity of an individual under surveillance is conveyed. The resulting data, approved for public viewing, is communicated in a network that employs the secure socket layer protocol and client authorization for network-level protection. Wickramasuriya *et al.* (Wickramasuriya, Datt & Mehrotra, 2006) present a privacy preserving video surveillance system that monitors subjects in an observation region using video cameras along with motion sensors and RFID tags. The motion detectors are used to trigger the video cameras on or off, and the RFIDs of the subjects provide authorization information in order to specify which individuals are entitled to privacy and hence have their visual information masked through image processing. More recently, Kundur *et al.* (Kundur, 2008) (Kundur, Luh, Okorafor & Zourntos, 2008) present the HoLiSTiC (Heterogeneous Lightweight Sensornet for Trusted Visual Computing) framework for WVSN security that exploits secure protocols in a hierarchical directional link communication network to achieve broadband low power communications. A decentralized visual secret sharing approach is used to preserve privacy.

Research has also emerged with the goal of assuring the authenticity of the data collected by sensor networks. When nodes are corrupted and provide false information, the entire network's legitimacy is compromised. The authentication of each node allows for the network to remain trusted. Several proposed solutions utilize common cryptographic concepts to provide such security. Feng *et al.* (Feng & Potkonjak, 2003) introduce a paradigm to cryptologically embed signatures into the collected data via watermarking techniques. Their objective is to efficiently watermark the data while introducing as little distortion as possible. Zheng et al. (Zheng, Li, Lee & Anshel, 2006) propose to offer authenticity assurance using a public key cryptographic scheme. A derivable public key scheme is used which has the effect of simplifying the cryptography and reducing the need for key storage, therefore making it more suitable for large scale sensor networks. Because these methods still increase the workload of the WSN, Martinovic *et al.* (Martinovic, Pichota & Schmitt, 2009) propose a novel paradigm that relies on the properties of wireless communications to provide authentication capabilities. They focus their study on taking advantage of frequency jamming to detect attacks and strengthen the WSN's security. Energy is always a concern when dealing with WSN where the nodes forming the network