Computers and Electrical Engineering 000 (2017) 1–18

Contents lists available at ScienceDirect

Computers and Electrical Engineering

journal homepage: www.elsevier.com/locate/compeleceng

Efficient compressed sensing-based security approach for video surveillance application in wireless multimedia sensor networks☆

S. Aasha Nandhini*, S. Radha

Department of ECE, SSN College of Engineering, Kalavakkam, India

ARTICLE INFO

Article history:
Received 14 June 2016
Revised 27 January 2017
Accepted 27 January 2017
Available online xxx

Keywords:
Compressed sensing
Security
Diagonal sum technique
Security keys
WMSN

ABSTRACT

Video surveillance application in wireless multimedia sensor networks (WMSNs) require that the captured video must be transmitted in a secured manner to the monitoring site. A compressed sensing (CS)-based security mechanism is proposed in which the security keys are generated from the measurement matrix elements for protecting the user's identity. The security keys are applied for protecting the video from being reconstructed by the attacker. The proposed framework is tested in real time using a WMSN testbed and the parameters such as memory footprint, security processing overhead, communication overhead, energy consumption, and packet loss are evaluated to demonstrate the effectiveness of the proposed security framework. The results showed that the proposed security mechanism has 92% less storage complexity compared to an existing CS-based security mechanism. The energy consumed for transmitting the secured measurements is 53% less when compared to raw frame transmission.

1. Introduction

A wireless multimedia sensor network (WMSN) basically consists of a few camera nodes and many regular nodes deployed in sensitive areas for surveillance applications like healthcare, home security, and intruder detection, traffic monitoring etc. Video surveillance application requires that the captured video must be transmitted in an efficient and secured manner to the monitoring site. For home security and intruder detection application, the camera is triggered whenever the motion is detected and the captured video is transmitted. It is necessary to ensure that the video is transmitted in a secure manner. Privacy is a major concern when dealing with sensitive applications where the identity of the person in the video requires protection [1]. It is sufficient to hide the region of interest from the attacker rather than the entire frame. The object present in the frame is detected and then the regions corresponding to the object alone is protected. Conventional encryption techniques require a huge amount of energy and memory for implementing the techniques in the nodes [2]. Compressed sensing (CS)-based security mechanisms can provide a high level of security by reducing the data transmission. CS states that the signal can be reconstructed with very few measurements using a nonlinear recovery process [3]. CS-based security mechanisms provide a high level of security but require more storage and energy complexity. Hence it is important

☆ Reviews processed and recommended for publication to the Editor-in-Chief by Guest Editor Dr. M. D. Selvaraj.
* Corresponding author.
E-mail addresses: aasha.nandhu@gmail.com (S.A. Nandhini), radhas@ssn.edu.in (S. Radha).

http://dx.doi.org/10.1016/j.compeleceng.2017.01.027
0045-7906/© 2017 Elsevier Ltd. All rights reserved.

to develop a CS-based security mechanism appropriate for WMSN that can provide a high level of security while reducing data transmission, storage and energy complexity.

The main contribution of the paper is to develop a simple and efficient security mechanism to protect the privacy of the video. An efficient selective block security (SBS) approach is proposed for preventing the attacker from extracting the compressive measurements. In this approach, CS is used for reducing the data transmission while security is taken care of with the help of the keys generated from the CS measurement matrix. The blocks corresponding to the objects are detected using a simple background subtraction method and block selection process (BSP). The performance of the proposed framework is evaluated using parameters such as memory footprint, security processing overhead, communication overhead, energy consumption, the percentage of reduction in samples and packet loss.

The rest of the chapter is organized as follows: Section 2 discusses the related works, Section 3 discusses the proposed SBS approach in detail. Section 4 discusses the performance evaluation. Conclusion and scope for future work are presented in Section 5.

2. Related works

A few CS-based security mechanisms available in literature are discussed in this section. The advantages and the limitations of those techniques are also given an emphasis.

In [3], the authors have explained in detail the basics and mathematics involved in CS and how it can be implemented in real time. They have motivated the design of new sampling schemes and devices that provide the information required for signal recovery using the smallest possible representation. Hence CS can be useful for WMSN applications dealing with a huge volume of data. However, the CS computation cost is slightly higher.

Recent developments in the security mechanisms related to interruption of data and privacy of data for monitoring applications have been explained by Gonçalves and Costa [4]. The authors have presented image cryptography which ensures the privacy of the image data. In addition to this, they have also discussed the authentication performed for watermarking and secure image monitoring issues.

Li et al. [5] have proposed a CS-based secure data transmission scheme in which encryption and decryption are carried out using the same set of keys at the transmitter and the receiver. The measurement matrix is generated at the transmitter based on the secret key while the encrypted measurements are transmitted for reconstruction. In this approach, different measurement matrices are generated for different keys, resulting in a higher storage overhead. The encoder design is simplified while transferring the complexity to the decoder side.

Tong et al. have used the CS scrambling process for protecting the privacy of the video. Privacy regions are scrambled through block-based CS sampling on quantized coefficients during compression. Security is ensured by a key controlled chaotic sequence which is used for constructing CS measurement matrix. The results showed that the scheme provides better security and good coding efficiency. Different keys generate different measurement matrices and hence the storage overhead is high [6].

Abhishek et al. [7] have proposed an effective algorithm in which the measurement matrix is generated using a pseudo-random generator. The initial seed for the pseudo-random generator is a secret random array which is highly chaotic and generated using piecewise linear chaotic map (PWLCM). If the initial condition, the system parameter and the number of iterations of PWLCM are concealed, it becomes impossible for the attacker to trace out the actual measurement matrix. The advantages of the method are reduced complexity, high level of security and good reconstruction quality. The algorithm performs well for publicly available datasets, however the proposed method is not tested on real-time sequences.

Agrawal and Vishwanath have adopted a compressive sensing framework for establishing secure physical layer communication over a Wyner wiretap channel. Compressive sensing can exploit channel asymmetry so that a message, encoded as a sparse vector, is decodable with high probability at the legitimate receiver while it is impossible to decode it with high probability at the eavesdropper. Wolfowitz secrecy and polynomial-time encoding/decoding algorithms are used for secret communication over the channel. The advantage of the proposed work is that it provides better accuracy, however, with no guarantee on the rate [8].

Zhao and Huang [9] have proposed a security scheme for wireless sensor networks (WSNs), which allows two legitimate nodes for establishing a common secret key by exploiting joint channel characteristics of the wireless channel. The established keys can then be used for constructing a measurement matrix and reconstruction matrix for the two nodes respectively. Analyses showed that the proposed scheme ensures a high level of security with less computational complexity for WSNs. However, the proposed scheme has high storage overhead and communication overhead.

Jin et al. [10] have addressed the energy constraint problem in WSN by proposing a hybrid security and data gathering scheme based on compressive sensing for multimedia data. The security solution consists of 8-bit integer chaotic block encryption and chaos-based message authentication codes. The compressed samples are encrypted using 8-bit chaotic block encryption while integrity is preserved using a message authentication algorithm. From the results, it is observed that the proposed solution decreases the complexity and energy consumption. However, the authors have not considered the memory constraint issue which is also a critical issue in WSN.

Ji et al. [11] have proposed a compressed sensing-based encryption scheme for distributed WSNs that provide both compression and encryption without any need for additional computational overhead. In this approach, the cipher text depends on a few randomized bits whose positions are determined by two keys. Unconditional security is guaranteed by the limited