Computers and Electrical Engineering 60 (2017) 175–192

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 8 February 2017

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/

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

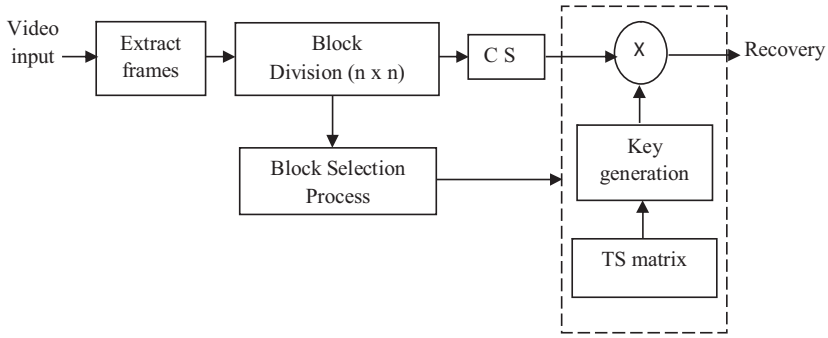

Fig. 1. Block diagram of selective block security approach.

memory capacity of the eavesdropper in this approach. From the results, it is observed that the approximation error of data decreases when the attacker compromises less number of sensor nodes. The proposed approach is simple and has a small memory footprint. However, the communication overhead is high due to sharing of random keys.

Wei et al. [12] have proposed a scheme to optimize the energy and distortion while providing a better encryption performance of multimedia content in WSN. A selective encryption approach was proposed to reduce the additional encryption overhead at the application layer. A resource allocation scheme was also proposed to improve the communication efficiency at the lower layers. From the results, it was observed that the proposed approaches achieve better video quality with a higher level of security and improved energy efficiency. However, the decoding latency occurs as the decoding of one frame depends on the other frames associated with the encryption block.

From the survey, it is observed that the CS-based security mechanisms can provide security as well as good compression performance. It is also observed that the existing CS-based security mechanisms provide better security, however, the storage and communication overhead is high. The compressive measurements of the captured video can be securely transmitted to the destination with the use of the efficient security mechanism. Thus, developing less complex CS-based security mechanism will be best suited for a resource constraint environment like WMSN.

3. Selective block security approach

A simple and efficient security mechanism is proposed to transmit the compressive measurements of the surveillance video in a secure manner. It is important to protect the privacy of the person in an indoor surveillance environment such as home, hospital etc. The attacker must not be able to get the information by eavesdropping the channel. Therefore, the values of the compressive measurements are transformed using a simple and novel technique called diagonal sum technique. The compressive measurements are transformed using keys generated from the elements of the measurement matrix which are stored in the sensor nodes. The compressive measurements of the video are transmitted after applying the security keys. These secured measurements protect the video from being reconstructed by the attacker for extracting the information. To reduce the complexity of the security approach, the security keys are applied only to the important regions of the video frame without degrading the security level. The key idea of this proposed approach is to use a single measurement matrix, unlike existing CS-based security mechanisms [5,6] in which different measurement matrices are used based on the predefined key values. In this work, measurement matrix is used for the compression as well as the security process. Fig. 1 shows the block diagram of the proposed SBS framework. In this framework block-based approach is adopted to reduce the computational complexity of the CS process [13,14]. The security is not applied to the entire video frame instead only to few blocks which represent the object or important region to be hidden.

The blocks that correspond to the object are detected by using a simple background subtraction process and BSP. The frames of size M x N are extracted from the video and divided into frames of size n x n to reduce the complexity of the CS process [15]. The frames undergo BSP to detect the blocks that correspond to the objects. CS is applied to all the blocks of the frame for obtaining the compressive measurements. The measurement process is carried out using the Toeplitz sensing (TS) matrix [16] and security keys are generated using a novel diagonal sum technique. The TS matrix requires less memory and energy complexity. Therefore, it is used to generate the security keys in this framework. The TS matrix requires $(2n^2 - 1)$ elements to generate the measurement matrix. Once the security keys are generated, they are applied to the compressive measurements for obtaining the secured measurements. These secured measurements are relayed through the sensor nodes to the destination where the compressive measurements are recovered using the same set of security keys generated at the source node. The complexity of the security process is reduced as the security keys are not applied to all the blocks of the frame but only to selected blocks to protect the privacy of the user from the eavesdropper.

Input: Differenced pixels dp_j where j represents the blocks.

Procedure:

Step 1: Compute the sum of the differenced pixels for all blocks $S_j = \sum_{i=1}^{N_1} dp_j(i)$ where S_j represents the sum of differenced pixels in the block j .

Step 2: The blocks which have the maximum sum is sorted

$$H_j = sort(S_j)$$

Where H_j represents the array of blocks with the maximum sum of pixels in descending order.

Output: ' L ' blocks with the maximum sum of pixels are selected based on a predefined threshold.

Fig. 2. Block selection process.

3.2.1. Block selection process

The BSP is a slight modification of the measurement selection process reported in [17]. The BSP is carried out by subtracting the input frames from the reference frame for obtaining the differenced measurements. Fig. 2 shows the BSP in detail.

Once the blocks with maximum sum of pixels are selected, the compressive measurements of those blocks alone are secured by applying security keys generated from the TS matrix.

3.2.2. Diagonal sum technique

In this technique, the keys are generated from the CS measurement matrix by using the matrix elements. The elements of the TS matrix are multiplied with the sum of the diagonal elements of the matrix to generate the key values. The total number of keys generated depends on the number of elements in the matrix and the diagonals of the matrix. Each key is used for each block to secure the compressive measurements. The keys are not applied to the entire frame and used without repetition for many blocks. The keys are generated using Eq. (1)

$$SK = mat_e * sum(diag(mat)) \tag{1}$$

where SK denoted the security keys and mat_e denotes the elements in the TS matrix where $e = 1, 2, ..., 127$. The total number of keys (T_k) that can be generated depends on the block size of the frame and is given in Eq. (2)

$$T_k = 2(2n_1{}^2 - 1) \tag{2}$$

where 'n_1' denotes the samples in the blocks of the frame. The CS by itself provides security as the attacker will not be able to know about the measurement matrix and, if at all the attacker knows about the measurement matrix also he will not be able to reconstruct without the security keys. The secured measurements are transmitted through the sensor nodes to the monitoring site for reconstruction using the orthogonal matching pursuit (OMP) algorithm. The OMP algorithm is a fast and inexpensive algorithm which goes through iterations to estimate the sparse vector [18]. The receiver also generates the same set of keys using the diagonal sum technique. Since the transmitter and the receiver have the same set of keys, perfect reconstruction of the transformed measurements at the receiver is possible. This approach provides better security with less complexity compared to other CS-based security mechanisms [5,6].

4. Performance evaluation

The performance of the security framework is evaluated in terms of storage overhead, energy consumption, communication overhead, security processing overhead, the percentage of reduction in samples and packet loss analysis. The simulations are carried out in MATLAB R2010a environment and the proposed work is experimentally validated using a WMSN testbed. The video sequences considered for implementation are ATM sequence, Hallway sequence and Stair sequence taken from IVY Lab Surveillance video dataset [19]. Two more captured video sequences, namely, corridor sequence 1 and corridor sequence 2, are also considered for implementation.

4.1. Simulation analysis

The frames of size 288×352 are extracted from the video and divided into blocks of size 8×8. The total number of samples in a block is denoted as $N_1 = 64$. The frames are subtracted from the reference frame for obtaining the difference frame to which BSP is applied to select the blocks corresponding to the object. CS is applied to all the blocks using the discrete cosine transform basis and the TS measurement matrix of size $M_1 \times N_1$ for obtaining the compressive measurements. The number of measurements per block is fixed at $M_1 = 30$ for analysis. The measurements are transformed using the security keys for transmitting the measurements in a secure manner. The total number of security keys generated from the TS matrix of size 64×64 is 16,380. To reduce the complexity of the security process, the security keys are applied only to few blocks that correspond to the object whose identity must be protected. After applying the security keys the measurements are transmitted for reconstruction. The same set of keys will be generated at the receiver side to retrieve the compressed measurements and the OMP algorithm is used to reconstruct the original frame.

4.1.1. Attack model

Initially, the attacker monitors the network to eavesdrop the communication and for extracting the information from the transmitted packets. With the SBS approach, the privacy of the video is protected with the security keys so that the attacker will not be able to reconstruct the video without the keys. It is assumed that the attacker is aware of the measurement matrix and sparsity level used in the network for processing the video data. Even though he has a prior knowledge of the matrix and sparsity level, he will not be able to reconstruct the frames as he is not aware of the security keys used in the network or the procedure to generate it. Fig. 3 shows the input frames of the video sequence taken from the database as well as the captured video sequence.

Fig. 4 shows the reconstructed frames using keys generated with the help of a diagonal sum technique at the receiver side.

It is observed from Fig. 4 that the security mechanism does not affect the quality of the reconstruction when reconstructed with the right key. Fig. 5 shows the video reconstructed by the attacker with the knowledge of sparsity level, measurement matrix and recovery algorithm. The blocks corresponding to the object are secured using the security keys so that even if the attacker captures the packet he will not be able to reconstruct the video properly without the knowledge of security keys. Hence the privacy of the video is protected by concealing the identity of the object. The video frames can be reconstructed with better accuracy at the receiver as both the source and destination nodes have the same set of keys.

4.1.2. Percentage of reduction in samples

The percentage of reduction in samples is calculated using Eq. (3)

$$P_s = \left(1 - \frac{P}{Q}\right) \times 100\% \tag{3}$$

where P represents the compressive measurements per frame and Q represents the total samples in a frame. The percentage of reduction in samples is computed from a various number of measurements per block at $M_1 = 20, 30, 40$. Fig. 6 shows the reduction in samples for different sets of measurements.

From Fig. 6 it is observed that as the number of measurements per block increases, the percentage of reduction in samples decreases.

4.2. Complexity analysis

The complexity of the proposed system is evaluated by considering parameters such as energy consumed for implementing the security mechanism, communication overhead, memory footprint, security processing overhead, encryption ratio and encryption time. The TelosB [20] nodes are considered for analysis and the SBS approach is implemented in the nodes. The CS-based security mechanisms reported in [5,6] require storing one key for each block and its corresponding measurement matrices. The complexity of this mechanism is high as it uses different measurement matrices based on the predefined keys. The security level is high with high storage and computational complexity.

4.2.1. Energy complexity

Energy consumption of the proposed approach is computed by considering the energy for diagonal sum technique, block selection process and SBS approach. The energy is computed for all the processes involved in the security framework using the energy consumption values for the basic operations involved in the MSP430 microcontroller which is given in Table 1.

(a) Key generation

The energy consumed for generating the keys from the measurement matrix elements stored in the node is computed using Eq. (4) as 50 µJ.

$$E_{kg} = 2 \times \sum_{d_1=1}^{N_1-1} (d_1) * e_{add} + (2N_1 - 1) \times (2N_1 - 1) * e_{mul} \tag{4}$$

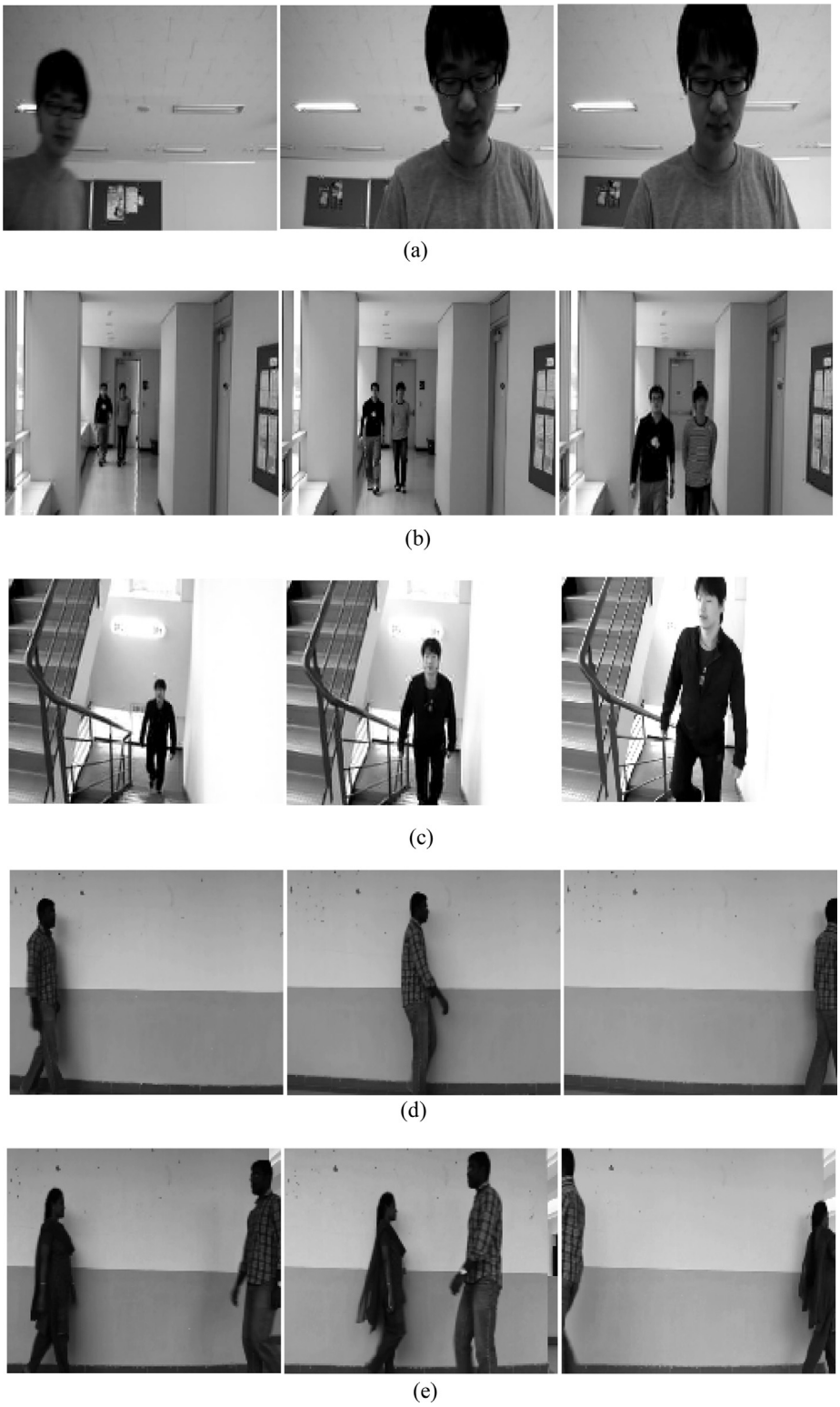

Fig. 3. Input frames of video sequences a) ATM, b) hallway, c) staircase, d) corridor sequence 1, e) corridor sequence 2.

Fig. 4. Frames reconstructed by at the destination using the right key a) ATM, b) hallway, c) staircase, d) corridor sequence 1, e) corridor sequence 2.

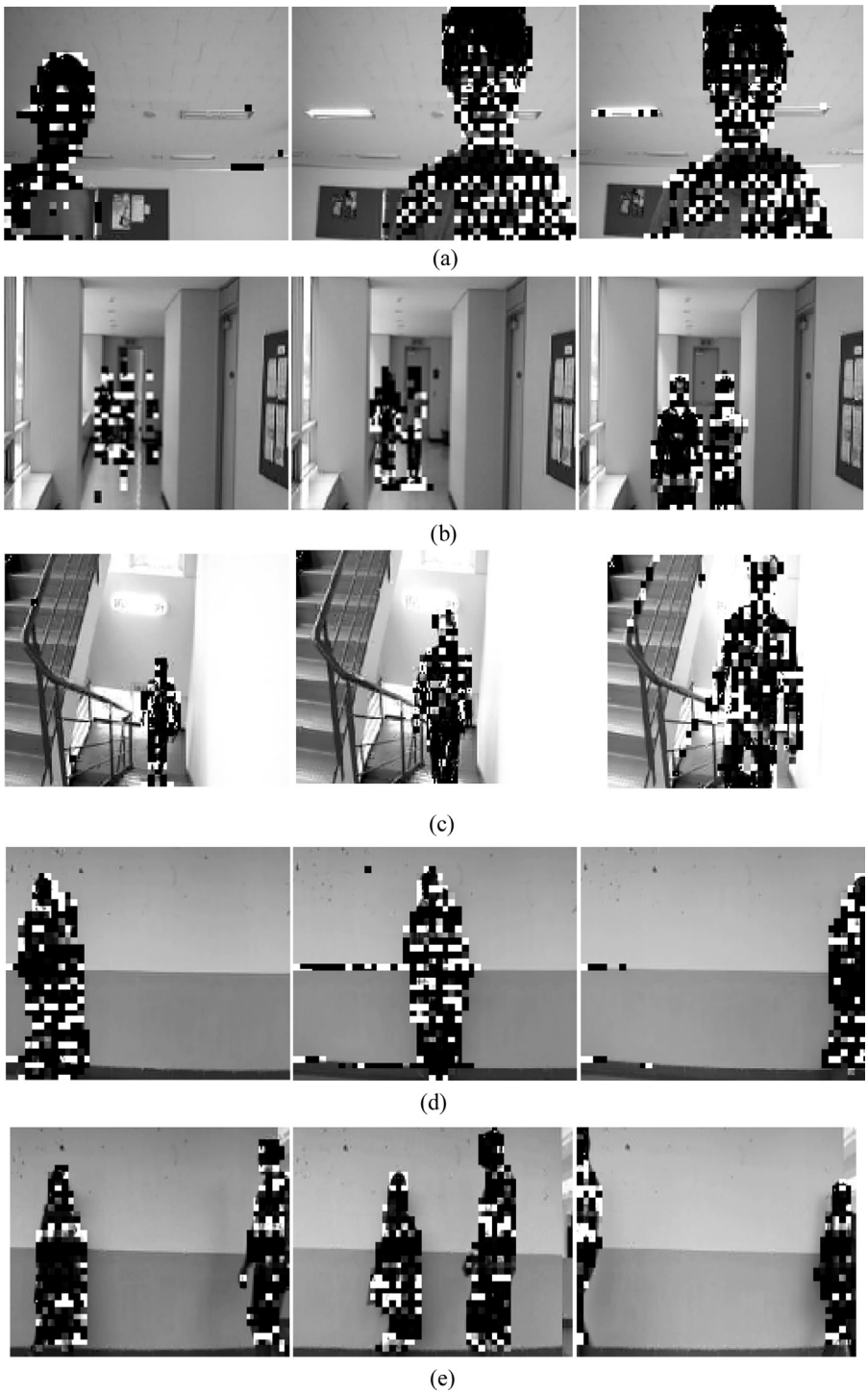

Fig. 5. Frames reconstructed by the attacker using wrong key a) ATM, b) hallway, c) staircase, d) corridor sequence 1, e) corridor sequence 2.

(b) Block selection process

The BSP is carried out by subtracting the current frame blocks from the reference frame blocks. The blocks with the maximum sum of pixels are selected for the security process. The energy for BSP process is calculated using Eq. (5) as 147 µJ

$$E_{BSP} = [N_1 * e_{sub} + (N_1 - 1) * e_{add}] \times B_N \tag{5}$$

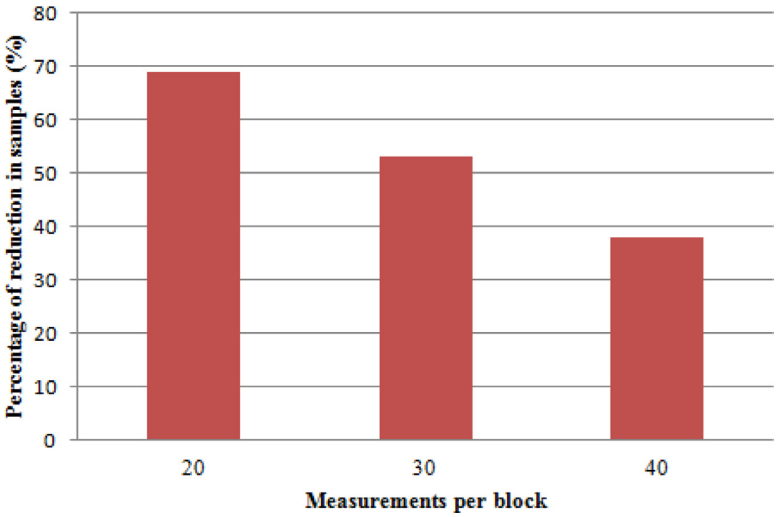

Fig. 6. Percentage of reduction in samples.

Table 1
Energy consumed by the MSP430 microcontroller [21].

Variable	Operation performed	Energy consumed
e_{add}	Addition over 1 byte	0.73 nJ
e_{sub}	Subtraction over 1 byte	0.73 nJ
e_{mul}	Multiplication over 1 byte	2.92 nJ
e_{shift}	Shift over 1 byte	0.73 nJ
e_{read}	Reads 1 byte from the flash memory	8.2 µJ
e_{write}	Writes 1 byte to the flash memory	34.9 µJ

where N_1 is the total number of samples in a block and B_N represents the number of blocks in a frame.

(c) SBS approach

The energy consumed for the processes involved in the SBS approach is given below.

i) CS process

The energy consumed for applying CS for a video frame is computed as 3.345 J using Eq. (6)

$$E_{CS} = [[n^2(n-1) + M_1(n^2-1)] * e_{add} + [n^3 + M_1 n^2] * e_{mul} + 2n^2 * e_{read} + M_1 * e_{write} + 127 * e_{read} + 127 * e_{write}] * B_N \quad (6)$$

ii) Security mechanism

The energy consumed for applying keys to the compressive measurements is computed as 88 µJ using Eq. (7)

$$E_{SM} = M_1 * e_{mul} * B_s \quad (7)$$

where M_1 is the number of measurements per block and B_s represents the total number of blocks selected using BSP.

4.2.2. Security communication overhead

In the proposed security framework, there is no communication overhead as the security approach does not require any overhead to be transmitted before the message. The transmitter and receiver have the same set of measurement matrix elements to generate the keys in SBS approach. The existing CS-based security mechanisms require the keys to be shared between the entities to generate the same measurement matrix based on the keys [5,6].

4.2.3. Memory footprint

a) Selective block security approach

The proposed security mechanism requires the elements of the measurement matrix to be stored in the node for generating the security keys. In this framework 127 elements are stored for generating the measurement matrix and hence the memory footprint of the SBS approach is 127 bytes which make it feasible in TelosB node which has 10 K RAM [20]. Existing CS-based security mechanisms [5,6] require 1584 bytes of storage space for storing the security keys per frame, resulting in a 92% increased complexity compared to the proposed SBS approach. The existing CS-based security mechanisms also require different matrices for different keys leading to higher storage overhead.

Table 2
Time consumed by the MSP430 microcontroller for different operations [21].

Variable	Operation performed	Time consumed
t_{add}	Addition over 1 byte	1 µs
t_{sub}	Subtraction over 1 byte	1 µs
t_{mul}	Multiplication over 1 byte	4 µs
t_{shift}	Shift over 1 byte	1 µs
t_{read}	Reads 1 byte from the flash memory	2.69 ms
t_{write}	Writes 1 byte to the flash memory	4.49 ms

Table 3
Key generation Process.

Number of elements stored in the measurement matrix	Security processing overhead (ms)	Energy consumption (µJ)	Memory footprint (bytes)
127	69	50	127

Table 4
Encryption ratio and Encryption time for different input video.

Input video	Encryption ratio	Encryption time (µs)
ATM	0.31	2100
HALL	0.135	1100
STAIR	0.23	1400
Corridor sequence 1	0.054	516
Corridor sequence 2	0.124	1000

4.2.4. Security processing overhead

Security processing overhead is computed by calculating the time taken for processing the security mechanism in the sensor node. The time consumed for the basic operations to be performed on the nodes is given in Table 2.

The time taken for generating the keys is given in Eq. (8)

$$T_{kg} = 2 \times \sum_{d_1=1}^{N_1-1} (d_1) * t_{add} + (2N_1 - 1) \times (2N_1 - 1) * t_{mul} \tag{8}$$

The time taken for multiplying the keys with the compressed measurements is given in Eq. (9)

$$T_{SM} = M_1 * t_{mul} * B_s \tag{9}$$

where B_s denotes the blocks corresponding to the object. The total security processing overhead is the sum of the processing time of the key generation and value transformation processes which is computed as 0.2 s using Eq. (10)

$$SPO = T_{kg} + T_{SM} \tag{10}$$

The energy and storage complexity of the key generation process depends on the block size 'n' and not on the measurements 'M_1'. Table 3 shows the evaluation of the diagonal sum technique.

4.2.5. Encryption ratio and encryption time

Encryption ratio measures the ratio between the number of encrypted blocks and the total number of blocks in a frame [22]. Encryption time measures the time taken to encrypt the selected blocks per frame. Table 4 shows the encryption ratio and the encryption time for different input videos. It is observed that the encryption time is proportional to the encryption ratio. The encryption ratio of selective encryption is 83% less compared to the full encryption process resulting in less energy and complexity.

4.3. Implementation in a WMSN testbed

The performance of the security mechanism is evaluated experimentally using a WMSN testbed by transmitting the measurements in a secured manner from the source to the destination. A WMSN testbed consists of WingZ gateway and TelosB nodes which act as the source node and relay nodes respectively. WingZ is a highly capable sensor node that can be used for processing the multimedia data and CS-based algorithms. The compressive measurements obtained from the WingZ node are transmitted via the TelosB nodes to the PC which is present at the monitoring site. The CS-based SBS approach is implemented in a testbed.

Fig. 7. WingZ source node.

4.3.1. WMSN testbed

A WMSN testbed has a WingZ sensor node and TelosB nodes. The WingZ node is used as the source node while the TelosB nodes are used as the relay nodes. WingZ stands for Wireless IP Network Gateway for ZigBee which is shown in Fig. 7. It is a single board computer based on Texas Instruments Open Multimedia Application Platform with various feature rich peripherals and multiple wireless and wired network interfaces. This device is highly flexible and configurable in terms of usage and applications perspective. WingZ has a 720 MHz ARM Cortex A8 processor, integrated 520 MHz DSP with video Accelerator, 256 MB RAM and 512 MB NAND Flash Memory, Onboard Micro-SD interface, CC2520 and CC2531 radio module [23].

WingZ is operated in the Linux environment using C programming. The WingZ gateway has an Ethernet port, which extends its use for the internet of things (IOT) applications. An 8 GB SD card is used to process efficient algorithms and to store a large volume of data. It has a touch screen which can be accessed on a PC using PuTTY. Various connectors are available on the WingZ-Energy board to connect the peripherals. A 5 V DC power adapter is used to power the WingZ node. A camera module is attached to the WingZ source node to capture the video and process it using the algorithm implemented in the WingZ hardware. WingZ can be used as a small computer by connecting a keyboard and mouse to it. WingZ can communicate with the TelosB nodes using serial communication, which can further communicate with other TelosB nodes using the ZigBee CC2420 module.

The TelosB nodes [20] are operated under the ContikiOS platform [24] an embedded operating system specifically designed for wireless sensor network. The WingZ node can be operated under a Linux (Angstrom, Ubuntu, Fedora), Android (Gingerbread, ICS) and Windows (WinCE) platform.

4.3.2. Experimental setup

The CS-based SBS framework is tested using the WMSN testbed in a lab environment as shown in Fig. 8. The network is modeled using the WingZ node and TelosB node, where WingZ acts as the source node in which the source algorithm is executed. The PC acts as the destination at the monitoring site. The TelosB nodes are randomly deployed between the source and the destination for relaying the measured event. For the experimental purpose, the captured video is stored in the WingZ and the source algorithm is implemented for obtaining the compressed measurements. These measurements are transmitted through the relay nodes. The video is reconstructed at the monitoring site from the received measurements using MATLAB.

The TelosB node is attached to the WingZ node as shown in Fig. 9 to transmit the compressed measurements through ZigBee module CC2420. The packets reach the destination node attached to a PC. The received CS measurements are used to reconstruct the video in MATLAB environment.

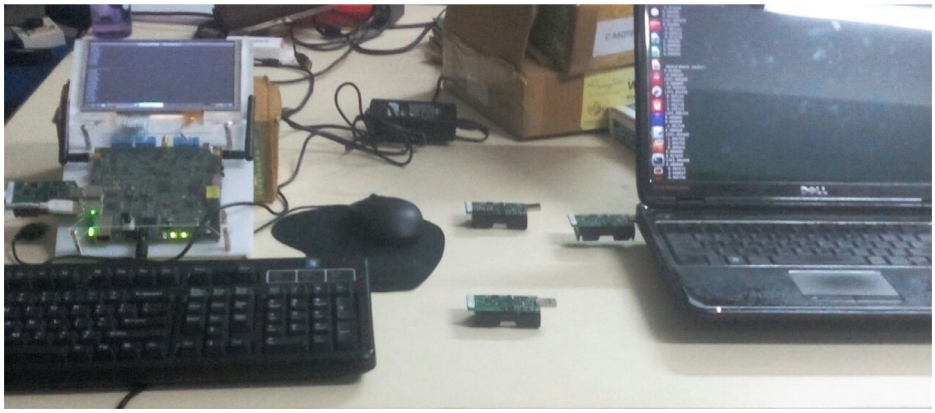

Fig. 8. Experimental set up.

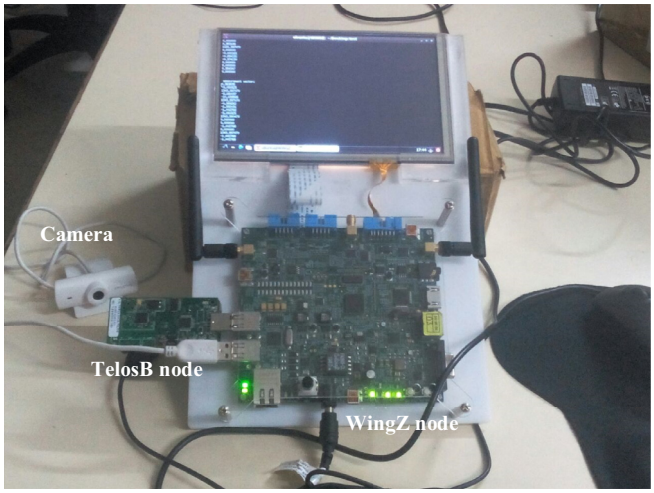

Fig. 9. WingZ node with TelosB attached.

Block number P =1 to B_N (1 byte)	SB=0 or 1 0 – Not secured 1- secured block (1 byte)	Secured measurements (M_1) (M_1 bytes)

Fig. 10. Packet structure.

4.3.3. Experimental results

The input video sequences (ATM, hallway, stairs, corridor sequence 1 and corridor sequence 2) considered for implementation in the WingZ node are shown in Fig. 3. Only one frame is considered for demonstration. The CS is implemented using the DCT and TS matrix. The frames of size 288×352 are extracted from the video which is given as input to the source node. The proposed frameworks are implemented in the source node for obtaining the measurements. The compressive measurements are transmitted through the network and the packet size can be varied and the maximum number of bytes that can be sent through a packet is 127 bytes. Fig. 10 shows the structure of the packet, where the first field represents the block number and the second field is used to identify the secured block.

Programming is done using the high-level C language and OpenCV is used to read the video and extract the frames from the video. OpenCV is used mainly in the field of computer vision. The proposed framework is implemented using C programming language. The TelosB nodes are configured as a transmitter and receiver using the C language and protothreads in the ContikiOS OS platform. Fig. 11 shows the WingZ node displaying the measurement vector obtained using the CS algorithm dumped in the node.

The node that is configured as the transmitter is attached to the WingZ, which forwards the measurements to another TelosB present within its transmission range. The transmission of measurements through the TelosB nodes is shown in Fig. 12.

Fig. 11. WingZ with measurement vector displayed in LCD.

```
root@instant-contiki: /home/user/contiki-2.6/examples/rime
File  Edit  View  Search  Terminal  Help
029  4841  2058  511  828  -2447  3804  -1377  2531  -1333  -4130  2527  879  95
5  9012  1648  2329  2233  5213  -2463
1460534725 Channel set to 16
1460534725 1.0: Received packet from 2.0, hops 1
1460534725 Receiver: Packet has been received [5] Packet Data is:
1460534726 5  -2866  1545  -1957  -1374  3101  -2861  4590  -3030  1431  3012  -6249  -416  -1083  -1728  -659  3685  -3691  2353  -2854  820  3236  -2
608  -1108  1835  -5975  -155  -1535  -85  -3253  3714
1460534733 Channel set to 4
1460534733 1.0: Received packet from 2.0, hops 1
1460534733 Receiver: Packet has been received [6] Packet Data is:
1460534733 6  -33  16  -16  -22  32  -15  37  -25  17  37  -71  -32  -17  -7  -6  28  -34  16  -24  10  37  -25  -7  0  -77  -10  -16  -15  -44  28
1460534738 Channel set to 9
1460534738 1.0: Received packet from 2.0, hops 1
1460534738 Receiver: Packet has been received [7] Packet Data is:
1460534738 7  -33  16  -16  -22  32  -15  37  -25  17  37  -71  -32  -17  -7  -6  28  -34  16  -24  10  37  -24  -7  0  -77  -10  -16  -15  -43  28
1460534744 Channel set to 6
1460534744 1.0: Received packet from 2.0, hops 1
1460534744 Receiver: Packet has been received [8] Packet Data is:
1460534744 8  -33  16  -16  -22  32  -15  37  -25  17  37  -71  -32  -17  -7  -6
  28  -34  16  -24  10  37  -24  -7  0  -77  -10  -16  -15  -44  28
1460534749 Channel set to 15
1460534749 1.0: Received packet from 2.0, hops 1
1460534749 Receiver: Packet has been received [9] Packet Data is:
1460534749 9  -32  16  -16  -21  32  -15  36  -25  17  36  -70  -32  -17  -7  -6
  28  -33  16  -23  10  36  -24  -7  0  -76  -10  -16  -15  -43  27
1460534755 Channel set to 7
1460534755 1.0: Received packet from 2.0, hops 1
1460534755 Receiver: Packet has been received [10] Packet Data is:
1460534755 10  -32  16  -16  -21  31  -14  36  -24  17  36  -69  -31  -16  -7  -
6  27  -33  16  -23  10  36  -24  -7  0  -75  -10  -16  -14  -42  27
```

Fig. 12. Measurements received by the TelosB nodes acting as the relay node.

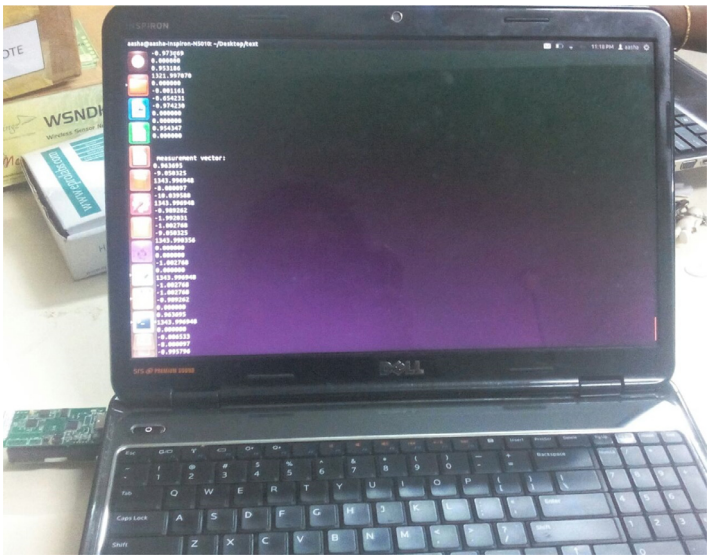

Fig. 13. Measurements displayed in a PC at the receiver side.

Table 5
Energy for basic operations involved in ARM Cortex A8 processor.

Notation	Operation	Energy consumed
we_{add}	Addition	6.5 nJ
we_{sub}	Subtraction	6.5 nJ
we_{mul}	Multiplication	0.013 µJ
we_{write}	Write	0.02 µJ
we_{read}	Read	0.013 µJ

The communication takes place with the help of the CC2420 radio model using one of the 16 frequency channels and the operating frequency of the TelosB nodes is 2.4 GHz. From the snapshot, it is observed that the node 1 receives secured measurements from node 2 and the number of hops is also shown. Fig. 13 shows the setup of a TelosB node connected to the PC. This node acts as the destination node and the secured measurements received are viewed on a PC. Further, these measurements are used for reconstruction in MATLAB.

Fig. 14 shows the reconstructed sequences with the right key on the PC using MATLAB from the measurements received.

The secured measurements obtained from the WingZ node are transmitted through the TelosB nodes. The destination node also has the same set of keys and, therefore, the compressive measurements are retrieved. In case an attacker tries to intercept the communication, he will not be able to properly retrieve the compressive measurements without the key. Fig. 15 shows the reconstructed sequence using the wrong key by the attacker. The identity of the user is protected by employing the SBS approach in the nodes.

4.3.4. Energy complexity analysis

Energy complexity analysis of the framework is carried out in the WMSN testbed considering the energy and time for the basic operations to be carried out in the ARM cortex A8 processor as given in Table 5. The energy complexity for implementing the proposed frameworks is computed by calculating the energy consumed for individual processes carried out in the WingZ node.

(a) CS-based SBS framework

The energy consumed for applying CS to the frame is given in Eq. (11). The energy for the CS process includes the energy for generating the measurement matrix also.

$$E_{CS} = [n^2(n-1) + M_1(n^2-1)] * we_{add} + [n^3 + M_1 n^2] * we_{mul} + 2n^2 * we_{read} + M_1 * we_{write} + 127 * we_{read} + 127 * we_{write}] * B_N \quad (11)$$

The energy for key generation process, block selection process and security mechanism are computed using Eqs. (12)–(14)

$$E_{KG} = 2 \times \sum_{d_1=1}^{N_1-1} (d_1) * we_{add} + (2N_1 - 1) \times (2N_1 - 1) * we_{mul} \quad (12)$$

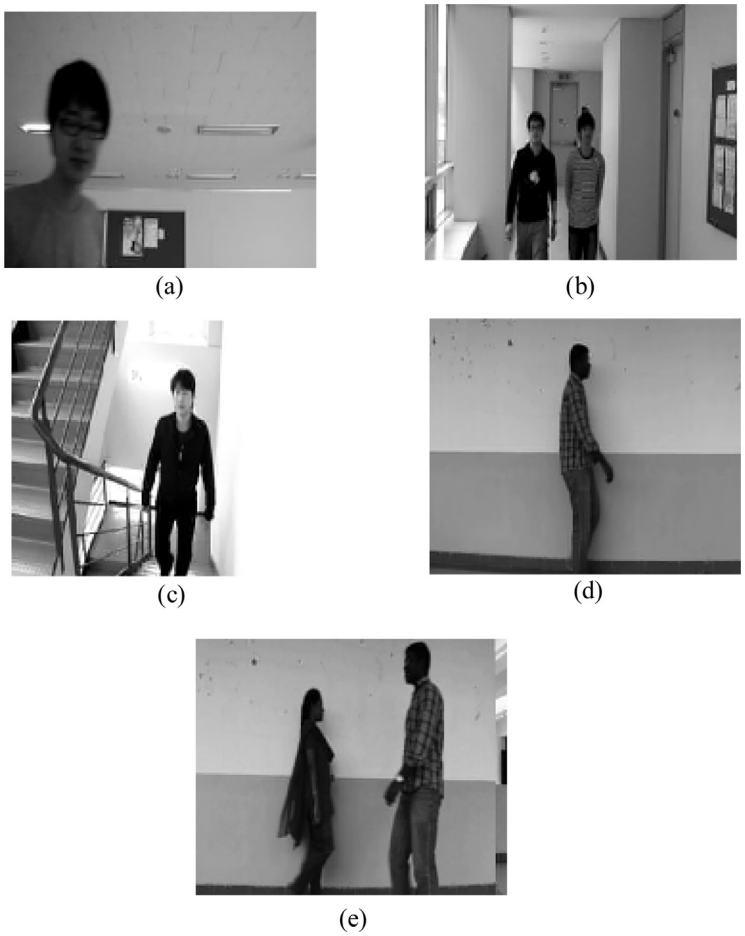

Fig. 14. Frames reconstructed by at the destination using the right key a) ATM, b) hallway, c) staircase, d) corridor sequence 1, e) corridor sequence 2.

$$E_{BSP} = [N_1 * we_{sub} + (N_1 - 1) * we_{add}] \times B_N \tag{13}$$

$$E_{SM} = M_1 * we_{mul} * B_s \tag{14}$$

The total energy consumed for the framework is computed using Eq. (15)

$$Total\ energy = E_{CS} + E_{KG} + E_{BSP} + E_{SM} \tag{15}$$

The total energy consumed for the framework is computed as 87 mJ using the Eq. (15).

(b) Communication energy

The communication energy is the sum of the transmission energy and reception energy. The transmission energy per bit (E_{tx}) is computed as 0.23 µJ [25]. The reception energy per bit is computed using Eq. (16)

$$E_{rx} = (t * I_r * V)/1024\ J \tag{16}$$

where the values of t, $I_{r,}$ and V are taken from the TelosB datasheet [20]. The energy for receiving per bit is calculated as 0.27 µJ. The communication energy per frame is computed as 190 mJ theoretically using Eq. (17).

$$E_f = B_M * (E_{tx} + E_{rx}) \tag{17}$$

where B_M represents the number of bits to be transmitted. The communication energy is computed using the TelosB node with the help of the powertrace tool [24] in ContikiOS. The communication energy per frame at the relay node is computed as 220 mJ. The communication energy for raw frame transmission is computed as 406 mJ using Eq. (17). The communication energy consumed for transmitting the secured measurements is 53% less compared to raw frame transmission.

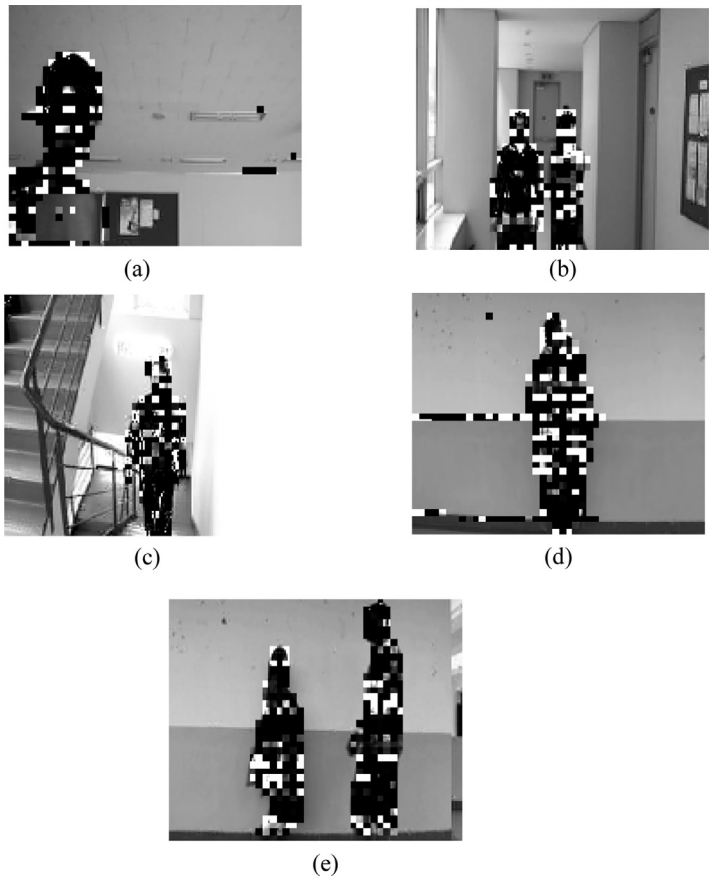

Fig. 15. Frames reconstructed by the attacker using wrong key a) ATM, b) hallway, c) staircase, d) corridor sequence 1, e) corridor sequence 2.

Table 6
Packet loss analysis of SBS approach with VCS framework.

Distance (d) (m)	Packet size	Total packets	Packet loss (%)	Percentage of recovery (%)
1	30	1584	0	100
5	30	1584	2.1	97.9
10	30	1584	3	97

4.3.5. Packet loss analysis

The packet loss analysis is carried out by calculating the ratio of the number of packets successfully received at the sensor node to the total number of packets transmitted at the source node. The experiment is carried out by varying the distance between the source node and the destination node while the relay nodes are randomly deployed between them. The packet loss is analyzed for d = 1, 5, 10 m. Table 6 shows the packet loss analysis of SBS approach.

From Table 6 it can be evident that as the distance between the source node and destination increases the packet loss also increases. The total packets refer to the number of blocks in the frame and the packet size refers to the number of measurements per block. From the results, it is observed that the proposed CS-based SBS approach is a practically feasible solution for video surveillance application in WMSN.

5. Conclusion and scope for future work

Since the WMSN-based video surveillance system can be used in private places like home and for patient monitoring in hospitals, it is necessary to protect the privacy of the person in the video. Hence, efficient selective block security approach is proposed for concealing the identity of the person in the video in case the attacker eavesdrops the communication. The security keys are generated based on the measurement matrix elements and are used to secure the compressed measurements. The attacker will not be able to reconstruct the video without the security keys even if he knows the sparsity level, measurement matrix and recovery algorithm. The SBS approach has 92% less storage complexity compared to the existing

technique. The encryption time for SBS approach is 83% less compared to full encryption time of the frame. The energy consumed for transmitting the secured measurements is 53% less compared to the raw frame transmission.

The proposed CS-based frameworks are tested in WMSN testbed consisting of WingZ as the source node and TelosB nodes as the relay nodes. The source algorithm is implemented in the WingZ and the measurements obtained in the WingZ are transmitted to the PC at the destination through TelosB nodes in a multihop manner. The frames were reconstructed from the received measurements using MATLAB. The packet loss analysis was carried out for the relay nodes for different distances. The percentage of recovery decreases as the distance between the source node and destination node increases.

References

[1] Ye Y, Ci S, Katsaggelos AK, Liu Y, Qian Y. Wireless video surveillance: a survey. IEEE Access 2013;1:646–60.
[2] Qi J, Hu X, Ma Y, Sun Y. A hybrid security and compressive sensing-based sensor data gathering scheme. IEEE Access 2015;3:718–24.
[3] Donoho DL. Compressed sensing. IEEE Trans Inform Theory 2006;52:1289–306.
[4] Gonçalves DdO, Costa DG. A survey of image security in wireless sensor networks. J Imag 2015;1(1):4–30.
[5] Li G, Wang Y, Lou Y. Secure data transmission scheme based on compressive sensing theory. J Comput Inf Syst 2013;9(20):8021–8.
[6] Tong L, Dai F, Zhang Y, Li J, Zhang D. Compressive sensing based video scrambling for privacy protection. In: Visual communications and image processing (VCIP); 2011. p. 1–4.
[7] Abhishek O, George SN, Deepthi PP. PWLCM based image encryption through compressive sensing. In: 2013 IEEE recent advances in intelligent computational systems (RAICS). IEEE; 2013. p. 48–52.
[8] Agrawal S, Vishwanath S. Secrecy using compressive sensing. In: ITW; 2011. p. 563–7.
[9] Zhao J, Huang J. Compressed sensing applied to wireless sensor networks security. In: Proceedings of the 2012 international conference on computer application and system modeling. Atlantis Press; 2012.
[10] Qi J, Hu X, Ma Y, Sun Y. A hybrid security and compressive sensing-based sensor data gathering scheme. IEEE Access 2015;3:718–24.
[11] Wu J, Liang Q, Zhang B, Wu X. Security analysis of distributed compressive sensing-based wireless sensor networks. In: The proceedings of the second international conference on communications, signal processing, and systems. Springer International Publishing; 2014. p. 41–9.
[12] Wang W, Hempel M, Peng D, Wang H, Sharif H, Chen H-H. On energy efficient encryption for video streaming in wireless sensor networks. IEEE Trans. Multimedia 2010;12(5):417–26.
[13] Song Y, Cao W, Shen Y, Yang G. Compressed sensing image reconstruction using intra prediction. Neurocomputing 2015;151:1171–9.
[14] Adler, A., D. Boublil, M. Elad, and M. Zibulevsky. A deep learning approach to block-based compressed sensing of images. arXiv preprint arXiv:1606.01519 (2016).
[15] Gan L. Block compressed sensing of natural images. In: 15th international conference on digital signal processing; 2007. p. 403–6. 1–4 July.
[16] Rauhut, H. Circulant and Toeplitz matrices in compressed sensing. arXiv preprint arXiv:0902.4394 (2009).
[17] Aasha NS, Radha S. Compressed sensing based object detection and tracking system using measurement selection process for wireless visual sensor networks. In: IEEE international conference on wireless communications, signal processing and networking (WiSPNET); 2016. p. 1160–5. March.
[18] Joel AT, Gilbert AC. Signal recovery from random measurements via orthogonal matching pursuit. IEEE Trans Inf Theory 2007:4655–66 Dec..
[19] IVY Lab surveillance video dataset, Available: http://ivylab.kaist.ac.kr/demo/vs/dataset.htm.
[20] 'TelosB', http://www.memsic.com/userfiles/files/Datasheets/WSN/telosb_datasheet.pdf.
[21] Amiri, M. Measurements of energy consumption and execution time of different operations on Tmote Sky sensor nodes, 2010.
[22] Massoudi A, Lefebvre F, De Vleeschouwer C, Macq B, Quisquater J-J. Overview on selective encryption of image and video: challenges and perspectives. EURASIP J Inf Secur 2008;2008(1):1.
[23] Nanda K, Nayak K, Chippalkatti S, Rao R, Selvakumar D, Pasupuleti H. Web based monitoring and control of WSN using WINGZ (wireless IP network gateway for Zigbee). In: 2012 sixth IEEE international conference on sensing technology (ICST); 2012. p. 666–71.
[24] 'ContikiOS', http://www.contiki-os.org.
[25] Nandhini SA, Sankararajan R, Rajendiran K. Video Compressed sensing framework for wireless multimedia sensor networks using a combination of multiple matrices. Comput Electr Eng 2015;44:51–66.

Aasha Nandhini S., Ph.D. She is a senior research fellow at SSN College of Engineering, India. She received the B.E. degree in Electronics and Communication Engineering from Rajalakshmi Engineering College, India, in 2010, the M.E. degree in Communication Systems from SSN College of Engineering, India, in 2012 and the Ph.D. degree from Anna University, in 2016. Her research interests include security issues and compressive sensing in wireless sensor networks.

Radha S., Ph.D. She is a professor and Head of the Department of ECE, SSN College of Engineering, Chennai, India. She is the recipient of the IETE—S.K. Mitra Memorial Award (2006) from the IETE Council of India and the CTS-SSN Best Faculty Award (2007, 2009) for outstanding academic performance. Her research interests include security, architecture issues of mobile ad hoc networks, WSNs and cognitive radios.