Hindawi Publishing Corporation
Journal of Sensors
Volume 2015, Article ID 636297, 7 pages
http://dx.doi.org/10.1155/2015/636297

Research Article

Secure Data Fusion in Wireless Multimedia Sensor Networks via Compressed Sensing

Rui Gao,[1,2] Yingyou Wen,[1,2] and Hong Zhao[1,2]

[1] *College of Information Science and Engineering, Northeastern University, Shenyang 110819, China*
[2] *Key Laboratory of Medical Image Computing of Ministry of Education, Northeastern University, Shenyang 110819, China*

Correspondence should be addressed to Yingyou Wen; yingyou_wen@163.com

Received 12 September 2014; Accepted 21 March 2015

Academic Editor: Qing-An Zeng

The paper proposes a novel secure data fusion strategy based on compressed image sensing and watermarking; namely, the algorithm exploits the sparsity in the image encryption. The approach relies on l_1-norm regularization, common in compressive sensing, to enhance the detection of sparsity over wireless multimedia sensor networks. The resulting algorithms endow sensor nodes with learning abilities and allow them to learn the sparse structure from the still image data, and also utilize the watermarking approach to achieve authentication mechanism. We provide the total transmission volume and the energy consumption performance analysis of each node, and summarize the peak signal to noise ratio values of the proposed method. We also show how to adaptively select the sampling parameter. Simulation results illustrate the advantage of the proposed strategy for secure data fusion.

1. Introduction

With the rapid development of wireless communication technologies, wireless multimedia sensor networks (WMSNs) are flourishing research fields due to the availability of low cost hardware such as CMOS and CCD cameras and the transmission of different kinds of data such as still images, multimedia streaming, and audio [1]. WMSNs not only enhance existing sensor network applications such as tracking, home automation, and environmental monitoring but also will enable several new applications like traffic avoidance, enforcement and control systems, advanced health care delivery, and so on [2]. Nowadays, when more and more sensitive information is transmitted over the WMSNs system, security has caught the attention of the research community with increasing multimedia applications of sensors [3].

Still images are important parts in WMSNs and usually used in the transmission of event triggered observations during short periods of time. Therefore, it is very important to protect still images from unauthorized access. Image encryption is one of the ways to ensure security and convert original image to another image that is hard to understand. Moreover, sensor nodes suffer from many constraints, including limited energy performances, low computation capability, less computational complexity, susceptibility to physical capture, tremendous transmission of multimedia data, and the use of insecure wireless communication channels [4]. Due to these limitations, it is essential to maximize the lifetime of sensors by reducing data transmission. Image data fusion is efficient in power consumption, so it plays a positive role in the computationally constrained and resource-constrained wireless multimedia sensor nodes.

In this paper, we propose a novel application of compressive sensing, namely, a lightweight still image encryption model for WMSNs security. We build our design on ideas from compressive sensing and watermarking. By analyzing the fact that image signal in WMSNs holds large amount of redundancy information, we project the captured image to the transform domain using only a few significant coefficients. Moreover, we utilize the watermarking approach to achieve authentication mechanism. These sparse coding coefficients are then deciphered using a novel reconstruction algorithm to recover the original image signal. We exploit the highly sparse data of the sensor nodes to obtain accurate reconstruction with only a few measurements. The framework of the proposed algorithm is illustrated in Figure 1.

The key contributions of the paper are summarized as follows.

(i) The compressive sensing methods in signal domain and hierarchical fusion techniques are integrated for sensor data fusion, which is applied to wireless multimedia sensor networks.

(ii) An integrated image data fusion framework is proposed. The algorithm developed under this framework transmits effective volume of sensor data in different sensor nodes and extends the network lifetime.

This paper is organized as follows: Section 2 introduces the related work. In Section 3, we describe the redundancy analysis of still image and provide still image encryption and authentication model for WMSNs security. Then, the proposed scheme suggests data reconstruction scheme. Security analysis and performance evaluation are given in Section 4. Finally, Section 5 offers conclusions and future directions.

2. Related Work

Data fusion techniques for reducing the number of data transmissions by eliminating redundant information have been studied as a significant research problem. These studies have shown that data fusion in WMSNs may produce various trade-offs among some network related performance metrics such as energy, latency, accuracy, fault-tolerance, and security (Table 1). It can be classified into three categories according to the abstraction level of the sensor data: low-level fusion, medium-level fusion, and high-level fusion [5, 6].

Low-Level Fusion. It is also referred to as a signal value fusion. It combines several sources of raw data to produce new raw data. Wimmer et al. [7] suggested a combined analysis by descriptive statistics of image and video low-level descriptors for subsequent static SVM classification. This strategy also allowed for a combined feature-space optimization which would be discussed herein. Mieslinger et al. [8] proposed a new method for the adaption of satellite-derived solar radiation values to ground measured time-series that was developed. The method was tested at the two sites ESPSA and DZTAM and for the four satellite data providers DLR, EHF, GMS, and HC3. Wu et al. [9] presented a simplified analytical model for a distributed sensor network and formulated the route computation problem in terms of maximizing an objective function, which was directly proportional to the received signal strength and inversely proportional to the path loss and energy consumption. Low-level fusion can keep all knowledge for the final decision process and the ability of a combined value-space optimization. Gao et al. [10] proposed a similarity model and power model. The proposal scheme divided multimedia data into multiple different pieces and transmitted the effective pieces to the selected sensor nodes.

Medium-Level Fusion. It is also described as attribute level fusion. Attributes or features of an entity (e.g., shape, texture, and position) are fused to obtain a feature map that may be used for other tasks (e.g., segmentation or detection of an object). Wang and Yin [11] proposed a perceptual hashing-based robust image authentication scheme, which applied the distributed processing strategy for perceptual image hashes. The scheme protected multimedia data from unauthorized access but increased the energy consumption simultaneously. Fucai et al. [12] presented a novel partial dynamic reconfiguration image sensor node prototype for wireless multimedia sensor networks to transmit sensitive images. The method proposed in the paper enabled the partial dynamic reconfiguration to decrease the volume of data. Medium-level fusion

Table 1: The performance is measured by PSNR (dB).

Number of samples M	Peppers	Lena	Boats
2000	19.03	18.56	18.32
3000	22.34	21.23	21.16
4000	25.12	25.01	24.93
5000	28.20	28.02	28.09
6000	30.16	29.67	29.73

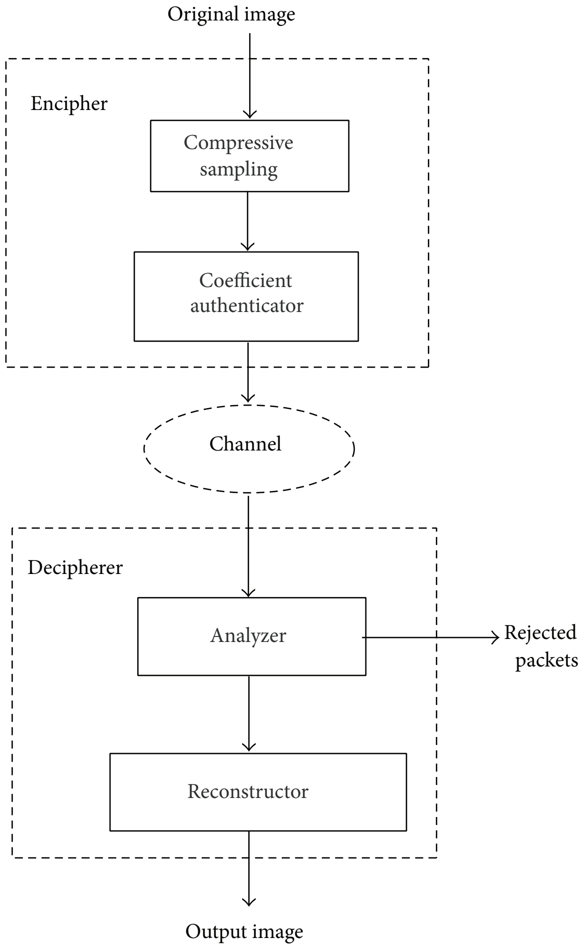

Figure 1: The framework of the algorithm.

reduces some information for the transmission process and achieves the combined attribute-space optimization.

High-Level Fusion. It is also known as decision level fusion. It takes decisions or symbolic representations as input and combines them to obtain a global decision. Blasch et al. [13] sought to describe MOEs for high-level fusion based on developments in Quality of Service and Quality of Information that supported the user and the machine, respectively. They defined HLF MOE based on information quality, robustness, and information gain. Costa et al. [14] proposed to address this issue with the use of highly expressive Bayesian models, which provided a tighter link between information coming from low-level sources and the high-level information fusion systems, and allowed for greater automation of the overall process. They illustrated the ideas with a naval HLIF system. High-level fusion needs higher artificial intelligence algorithm.

In short, secure data fusion has been incorporated into a wide range of existing sensor data. The crucial question is how to prolong the resource-constrained WMSNs lifetime to the longest time in secured mode. Thus, we analyze the advantages from different fields to build a novel image data fusion framework.

3. The Proposed Scheme

In this section, we explain the proposed scheme. We illustrate two stages in the proposed framework: still image encryption and decryption stages. The still image encryption stage gets several sources of image data and then projects the captured image data to the transform domain using only a few significant coefficients after analyzing the fact that image data in WMSNs holds large amount of redundancy information. In the decryption stage, we analyze the coherent measurements of image data from different sensor nodes. These measurements are then decoded using a novel reconstruction algorithm to recover the original image data.

3.1. Still Image Encryption. As everyone knows, WMSNs circumstance requires still images to minimize the energy consumption of data transmission as much as possible with security mode. The main target is how to securely and economically transmit the volume of image signal. Unlike common data, image signal in WMSNs usually holds large amount of redundancy information including spatial redundancy and surrounding redundancy [15], so the paper takes advantage of the characteristic to specify still image encryption model.

Spatial redundancy exploits the fact that an image very often contains strongly correlated pixels and the same brightness pattern repeated with statistic similarity [16]. The redundancy is explored by predicting a pixel value based on the values of its neighboring pixels. In addition, the availability of the same image block is represented by other blocks, due to the fact that light intensity and color in such areas are highly correlated. Thus, image represented by all pixel values suffers from a high level of spatial redundancy. The surrounding redundancy describes strongly correlated pixels of similar surroundings in different image signals. Natural images consist of separate areas indicating the object and its sceneries. We pay attention to the trends of the object in WMSNs and capture image signal containing the same surroundings. Thus, a high compression ratio can be achieved by eliminating these redundancies.

Compressive sensing has recently become very popular due to its interesting theoretical nature and wide area of applications [17]. Here, we consider compressive sensing in sensor data aggregation.

Suppose that x_i denotes image data of sensor node number i. Image data from sensor nodes is encoded by compressive sensing and is formally formulated as follows:

$$x = (x_1, x_2, \ldots, x_n) . \quad (1)$$

Suppose that the natural image $x_i \in R^N$ is K sparse on some basis Ψ and x_i can be represented by a linear combination of K vectors of Ψ with $K \ll N$. We have $x_i = \Psi\theta$, where Ψ is sparse matrix and θ is $N \times 1$ vector with only K nonzero entries. The measurement is described as $y_i = \Phi \cdot \widehat{\Psi} x_i$, where Φ is $M \times N$ matrix with $M \ll N$ and y_i represents the M measurements [17]. In WMSNs applications, the noise is present; we define y as

$$y_i = \Phi \cdot \widehat{\Psi} x_i, \quad i \in (1, n) . \quad (2)$$

According to the principle of discrete wavelet transform (DWT) sampling, the DWT coefficients to be measured should also cluster over low frequency bands. Typical measurements are chosen uniformly random. But, by placing the samples selectively but still in a random manner, we achieve better quality of image reconstruction. In this paper, we present a new sampling matrix designed in the frequency transform domain, which is applicable to the DWT. We define Φ as

$$\Phi = Q_M F W_N, \quad (3)$$

where F is the $N \times N$ diagonal matrix that is written as

$$F = \begin{bmatrix} F_f & & & \\ & F_f & & \\ & & \ddots & \\ & & & F_f \end{bmatrix}, \quad (4)$$

where F_f represents the $f \times f$ Fourier matrix. Q_M picks up columns of F randomly and W_N is a scrambling operator that randomly takes the N rows of $Q_M F$. Simply speaking, (2) takes the partial Fourier sampling over different frequency bands randomly. Obviously, we decrease the total amount of information to transmit and guarantee at the same time the expected security level. After compressive sampling, we utilize the authentication mechanisms to improve security and transmission efficiency. In the following, we discuss how to make the coefficient authenticator by watermarking approach.

Getting local time, we take the minute value m and second value s from WMSNs. The algorithm is shown in Figure 2.

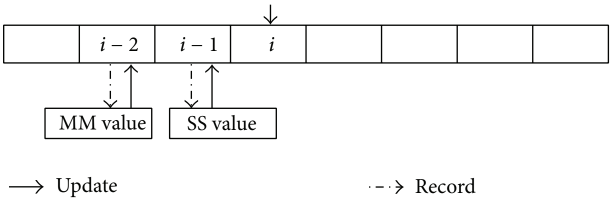

Figure 2: Authentication mechanism by watermarking approach.

Finding the ith sparse element in the y matrix, set the fact that$i = (m-1)\%M$, the $(i-1)$th element value is s, and the $(i-2)$th element value is m. In addition, record $(i-1)$th and $(i-2)$th element values. When the node receives the delivered package, it chooses the ith sparse element as a mark and decides the data integrity. Check $(i-1)$th and $(i-2)$th element values with the MM value and SS value of local time on WMSNs. If the values match, namely, $(i-1)$th element value is equal to the MM value and $(i-2)$th element value is equal to the SS value, update $(i-1)$th and $(i-2)$th element values. If $(i-1)$th element value is not equal to the MM value or $(i-2)$th element value is not equal to the SS value, the sensor node will reject the package.

3.2. Decryption Algorithm. In order to decrypt the image signal x from incoherent measurements y, we utilize l_1-optimization and min-TV solver. Obviously, we exploit the correlation of neighboring pixels and minimize the l_1 norm [18].

Considering the surrounding redundancy, we utilize the neighboring captured image signal $x_1, x_2, x_i, \ldots, x_n$ of x to reconstruct the signal x. The objective function is min $\|x\|_1$ and set equality constraint $y = \Phi \cdot \widehat{\Psi} x = \Theta \cdot x$. The Θ is shown as

$$\Theta^* = \arg\min \sum_i \left\| y_i - \sum_j \Theta_{ji}(x_i) \right\|_1, \quad (5)$$

where $y_1, y_2, y_i, \ldots, y_n$ are the measurement vectors of $x_1, x_2, x_i, \ldots, x_n$. Calculate the gradient x_k^* in every iteration $(x - x_k)^T (y - \Theta \cdot x_k)$, and x_{k+1} is shown as

$$x_{k+1} = x_k + \partial \left(x_k^* - x_k \right), \quad (6)$$

where ∂ is an adjustable parameter. According to the redundant constraints image signal, minimize the TV of the reconstructed signal to reconstruct image signal x again. The object function is as follows:

$$\mathrm{TV}(x) = \arg\min \left(\mathrm{TV}_1(x) + \mathrm{TV}_2(x) \right), \quad (7)$$

where TV represents the TV between the pixels of the natural image x and $\mathrm{TV}_2(x)$ represents the TV of the surrounding vector. Firstly, find the matching pixels of each pixel at different surrounding vector, calculate the partial derivative of current location, and modify the corresponding parameter. Change the parameter value that is less than the given threshold, until the minimal value.

In short, the algorithm for still image decryption is summarized in Algorithm 1.

4. Simulation Results

In this section, extensive simulations are provided to illustrate the effectiveness of the proposed methods. We first compare the total transmission volume of conventional encryption algorithm with the proposed scheme and then describe the energy consumption of every sensor node on single hop networks. Considering an encryption scheme, we present malicious node detection rate (DR) or false alarm rate (FAR) with the variation of the proportion of malicious nodes. Finally, we analyze the performance of the decrypted signal. We have developed a simulator based on MATLAB implementation to evaluate our proposed scheme. Assume that 50 sensors are deployed uniformly in 100 × 100 (m) network field and the radius of communication is 25 m. All the images are assumed sparse in the Daubechies-4 wavelet domain and have a spatial resolution of 256 × 256. For the still image encryption, we present results with $f = 16$.

Figure 3 shows the total transmission volume in different numbers of sensor nodes in WMSNs. Obviously, the proposed scheme provides less transmission volume than the exiting scheme [19]. The paper provides an energy-efficient transmission of still image signal. From simulation analysis, the amount of transmission volume is reduced by about 18.3% than the schemes without processing.

Due to still image encryption scheme, different sensor node makes different energy consumption. We analyze the security performance of still image encryption and authentication. For comparison purposes, suppose that 50 sensors deploy on signal hop network. Inspired by [19], Figure 4 shows the energy consumption of every sensor node. The 1st node consumes 1950 mA energy and the 2nd node takes up 2050 mA, while the average consumption of other nodes is 500 mA. The 1st and 2nd nodes consume significant energy, and then they accelerate the death time. But our scheme reduces the total energy consumption of the whole wireless multimedia sensor networks. Figure 5 describes the transmission volume of every sensor node. Our scheme provides less transmission volume in most of the sensor nodes except for the 1st and 2nd nodes. But our scheme reduces the total transmission volume.

Considering the security scheme, the paper analyzes the security performance of multimedia data transmission. Figure 6 describes the malicious node detection rate (DR) with the variation of the malicious nodes proportion. Our work supposes that attack probabilities are 0.02, 0.25, and 0.5. With the increase in the proportion of malicious nodes, the DR shows a slowly downward trend. When the proportion of malicious nodes is in the range [0, 0.25], we can obtain a higher malicious node detection rate. Figure 7 describes the false alarm rate (FAR) with the variation of the malicious nodes proportion. The paper supposes that attack probabilities are 0.02, 0.25, and 0.5. With the increase in the proportion of malicious nodes, the FAR continues with the upward trend correspondingly. When the proportion of malicious nodes is in the range [0, 0.25], the result achieves a low false alarm rate.

Considering the complexity of image data, we group scenarios into three different types: simple, general, complex.

```
Input: Encrypted images $x_1, x_2, x_i, \ldots, x_n$
Output: Decrypted image signal $y$
Procedure:
  (1) Initialization
      $x^* = \arg\min |\nabla x|_1$
  (2) Repeat following steps
      Update the matching surrounding $\Theta^*$
        $\Theta^* = \arg\min \sum_i \left\| y_i - \sum_j \Theta_{ji}(x_i) \right\|_1$
      Update the gradient of $x_k^*$
        $x_k^* = \arg\min (x - x_k)^T (y - \Theta x_k)$
      Update $x$ by following optimization
        $x^* = \arg\min |\nabla x|_1 + \sum_j \Theta_{ji}(x_i)$
      Until there is no much changes.
  (3) Minimize TV($x$)
      $\mathrm{TV}(x) = \arg\min (\mathrm{TV}_1(x) + \mathrm{TV}_2(x))$
```

Algorithm 1: Still image decryption.

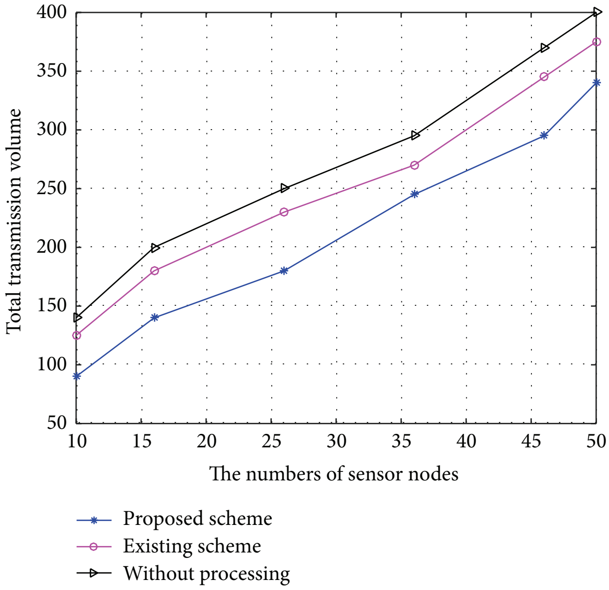

Figure 3: The total transmission volume of sensors nodes.

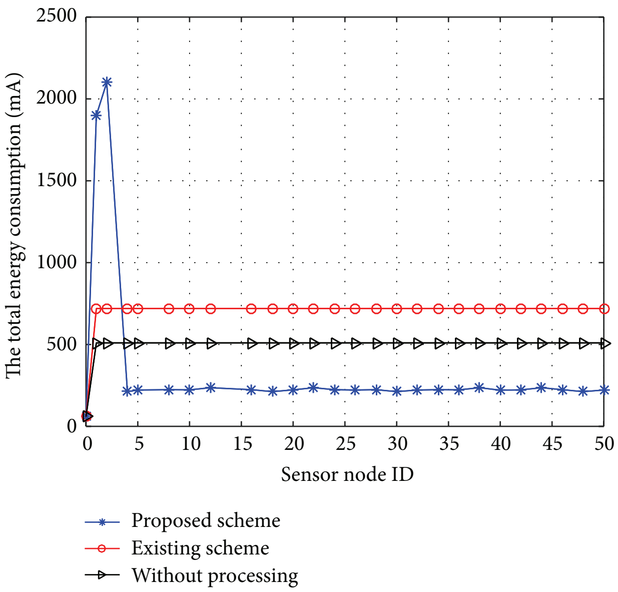

Figure 4: The energy consumption of every sensor node.

Figure 8 shows the MSE of the whole reconstructed image data from various scenarios. It can be observed that the image qualities of our proposed scheme, exiting scheme and the scheme without processing have errors in the process of compression and reconstruction during the data fusion. Along with the scene complexity increases, the proposed scheme makes more obvious immediate advantage.

Finally, to demonstrate the decryption practicality of the image signal, we apply it for three 256 × 256 images: Peppers, Lena, and Boats, and the data are collected from an average of ten runs. Table 1 summarizes the PSNR values when the number of measurements ranges from 2000 to 6000 (sampling ratio from 12.2% to 36.7%). Considering the limitation of bandwidth and power consumption, results of the measurements 6000 are even slightly better and the percentage of elements in our scheme is only 36.7%.

The simulations again show that the proposed still image encryption and authentication scheme consistently have better performance than other existing schemes. But some nodes consume significant energy and have a short life cycle.

5. Conclusion and Future Directions

This paper has proposed a secure conventional still image encryption algorithm. We develop an encryption algorithm

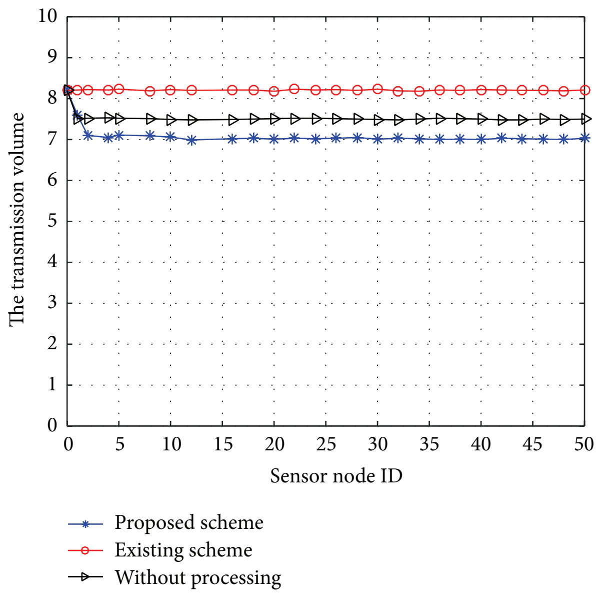

FIGURE 5: The transmission volume of every sensor node.

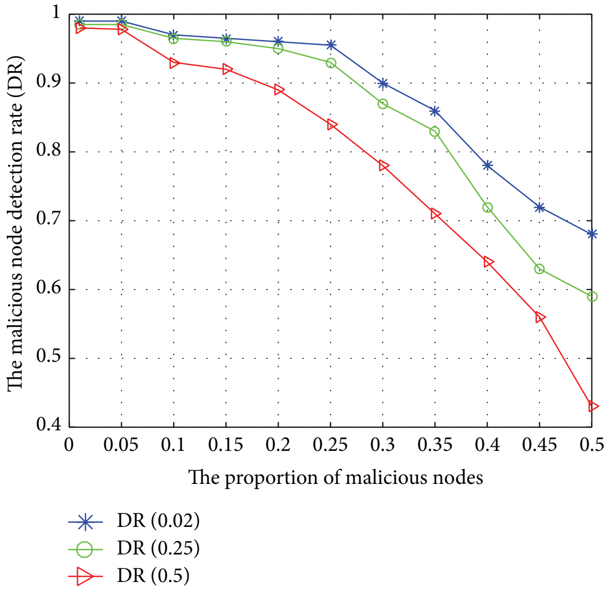

FIGURE 6: DR versus proportion of malicious nodes.

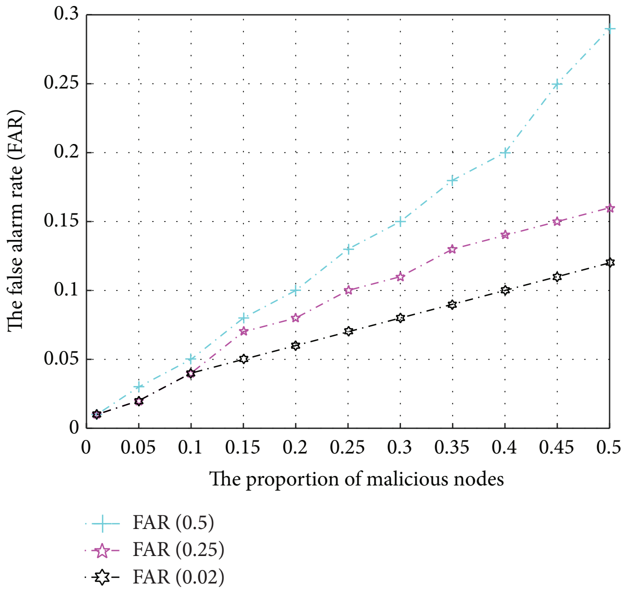

FIGURE 7: FAR versus proportion of malicious nodes.

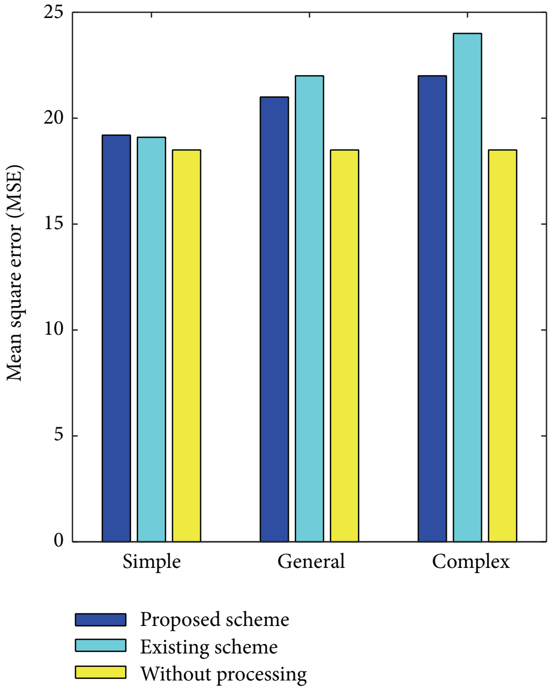

FIGURE 8: Mean square error of various scenarios.

based on compressed image sensing, which exploits the high degree of inherent sparsity in the natural images captured by sensor nodes and presents the fact that the image can be reconstructed using only a few acquisitions. We decrease the total amount of information to transmit and guarantee the expected security level. Moreover, the proposed design provides data authentication scheme that does not suffer from the influence of many existing malicious nodes. The proposed scheme has shown that the design transmits image signal securely and economically. In future work, we plan to extend our work to further improve compressive performance and conserve nodes energy.

Conflict of Interests

The authors declare that they do not have any commercial or associative interests that represent a conflict of interests in connection with the work submitted.

Acknowledgments

This work was supported by the Special Fund from the Central Collegiate Basic Scientific Research Bursary of China (Grant nos. 110818001 and 100218001) and in part by Grants from the National Natural Science Foundation of China (Grant nos. 60903159, 61173153, and 61300196).

References

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks," *IEEE Communications Magazine*, vol. 40, no. 8, pp. 102–114, 2002.

[2] I. F. Akyildiz, T. Melodia, and K. R. Chowdhury, "A survey on wireless multimedia sensor networks," *Computer Networks*, vol. 51, no. 4, pp. 921–960, 2007.

[3] G. Z. Manel, Z. Ruken, M. José, and B. Kemal, "The future of security in wireless multimedia sensor networks," *Telecommunication Systems*, vol. 45, no. 1, pp. 77–91, 2010.

[4] C. S. Deshmukh and S. V. Dhopte, "Network environment using compressive sensing technique of computer science and applications," *International Journal of Survey on Video Coding in Wireless Multimedia Sensor*, vol. 6, no. 2, pp. 13–17, 2013.

[5] E. F. Nakamura and A. A. F. Loureiro, "Information fusion in wireless sensor networks," in *Proceedings of the ACM SIGMOD International Conference on Management of Data*, pp. 1365–1371, June 2008.

[6] M. Guerrero-Zapata, R. Zilan, J. M. Barceló-Ordinas, K. Bicakci, and B. Tavli, "The future of security in wireless multimedia sensor networks," *Telecommunication Systems*, vol. 45, no. 1, pp. 77–91, 2010.

[7] M. Wimmer, B. Schuller, and D. Arsic, "Low-level fusion of image, video feature for multi-modal emotion recognition," in *Proceedings of the International Conference on Computer Vision Theory and Applications (VISAPP '08)*, pp. 145–151, Madeira, Portugal, January 2008.

[8] T. Mieslinger, F. Ament, K. Chhatbar, and R. Meyer, "A new method for fusion of measured and model-derived solar radiation time-series," *Energy Procedia*, vol. 48, pp. 1617–1626, 2014.

[9] Q. Wu, N. S. V. Rao, J. Barhen et al., "On computing mobile agent routes for data fusion in distributed sensor networks," *IEEE Transactions on Knowledge and Data Engineering*, vol. 16, no. 6, pp. 740–753, 2004.

[10] R. Gao, Y. Wen, H. Zhao, and Y. Meng, "Secure data aggregation in wireless multimedia sensor networks based on similarity matching," *International Journal of Distributed Sensor Networks*, vol. 2014, Article ID 494853, 6 pages, 2014.

[11] H. Wang and B. Yin, "Perceptual hashing-based robust image authentication scheme for wireless multimedia sensor networks," *International Journal of Distributed Sensor Networks*, vol. 2013, Article ID 791814, 9 pages, 2013.

[12] L. Fucai, J. Zhiping, and L. Yibin, "A novel partial dynamic reconfiguration image sensor node for wireless multimedia sensor networks," in *Proceedings of the IEEE 9th International Conference on Embedded Software and Systems*, pp. 1368–1374, 2012.

[13] E. Blasch, P. Valin, and E. Bosse, "Measures of effectiveness for high-level fusion," in *Proceedings of the 13th Conference on Information Fusion (FUSION '10)*, pp. 1–8, July 2010.

[14] P. C. G. Costa, K. B. Laskey, K. C. Chang, W. Sun, C. Y. Park, and S. Matsumoto, "High-level information fusion with bayesian semantics," in *Proceedings of the 9th Bayesian Modelling Applications Workshop*, 2012.

[15] C. Tang and C. S. Raghavendra, "Compression techniques for wireless sensor networks," in *Wireless Sensor Networks*, pp. 207–231, Springer, New York, NY, USA, 2004.

[16] S. K. Kil and J. S. Lee, "Lossless medical image compression using redundancy analysi," *International Journal of Computer Science and Network Security*, vol. 6, no. 1, pp. 50–56, 2006.

[17] D. L. Donoho, "Compressed sensing," *IEEE Transactions on Information Theory*, vol. 52, no. 4, pp. 1289–1306, 2006.

[18] l1-magic, http://www.l1-magic.org.

[19] E. J. Duarte-Melo and M. Liu, "Analysis of energy consumption and lifetime of heterogeneous wireless sensor networks," in *Proceedings of the IEEE Global Telecommunications Conference (GLOBECOM '02)*, vol. 1, pp. 21–25, Taipei, Taiwan, November 2002.

Journal of Engineering
The Scientific World Journal
International Journal of Rotating Machinery
Journal of Sensors
International Journal of Distributed Sensor Networks
Advances in Civil Engineering
Journal of Control Science and Engineering
Journal of Robotics
Journal of Electrical and Computer Engineering
Advances in OptoElectronics
VLSI Design
International Journal of Navigation and Observation
Modelling & Simulation in Engineering
International Journal of Aerospace Engineering
International Journal of Chemical Engineering
International Journal of Antennas and Propagation
Active and Passive Electronic Components
Shock and Vibration
Advances in Acoustics and Vibration