Given its importance, the problem of secure data aggregation in wireless multimedia sensor networks has attracted great attention in the literature. Wireless multimedia sensor networks present some challenges that are common to wireless sensor networks, such as the existence of limited resources, like sensors memory, energy consumption, and CPU performance. Many methods have been proposed to attempt to solve the problem. However, the existing data aggregations do not take into account the redundancy of the multimedia data. In order to improve the energy efficiency for multimedia data, we propose a similarity model and power model. The proposal scheme divides multimedia data into multiple different pieces, and transmits the effective pieces to the selected sensor nodes. Through theoretical justifications and empirical studies, we demonstrate that the proposed scheme achieves substantially superior performances over conventional methods in terms of energy efficiency and data transmission under the resource-constrained wireless multimedia sensor networks.

1. Introduction

A wireless sensor network consists of a large number of small, inexpensive, disposable, and autonomous sensor nodes which gather and summarize information from various applications and environments that are difficult for us to approach directly [1]. Research and development in wireless sensor networks are becoming increasingly widespread due to their low cost and low maintenance in deployment. Wireless multimedia sensor networks (WMSNs) enable the transmission of different kinds of data such as still images, multimedia streaming, and audio due to the availability of low cost hardware such as CMOS and CCD cameras. Thus, WMSNs are expected to be solutions to variety fields, such as environmental monitoring, military applications, disaster management, and advanced health care delivery [2].

WMSNs suffer from many constraints, including low computation capability, small memory, limited energy performances, susceptibility to physical capture, tremendous transmission of multimedia data, and the use of insecure wireless communication channels [3]. As the various applications of WMSNs increase, the problems of security are also complex. Secure data aggregation is efficient in power consumption, so it plays a positive role in the computationally constrained and resource-constrained wireless sensor nodes. Ideally secure data aggregation for WMSNs should have less computational complexity, have longer lifetime, and have less latency for data transmission from sensor nodes to sinks [4]. Due to these limitations, it is essential to maximize the lifetime of sensors by reducing the amount of information that traverses the network. The data aggregation that we present in this work is designed to comply with the above-mentioned characteristics of secure data aggregation.

In this paper, we propose a novel application of similarity matching, namely, a security-enhanced energy-efficient data aggregation for WMSNs security. We build our design on ideas from fuzzy similarity matching. By analyzing the fact that multimedia data in WMSNs involves large amount of similar information, we establish a similarity model and power model. Firstly we divide the multimedia data into multiple pieces and extract the feature from the different pieces. Then, comparing the difference between the pieces feature and the standard feature, we only present a few significant pieces in order to decrease the volume of multimedia data.
and transmit multimedia data efficiently. According to the standard data feature, we make the sensor node chooser for effective multimedia data and update the power value of sensor nodes. The framework of proposed algorithm is illustrated in Figure 1.

This paper is organized as follows. In Section 2, we overview the existing secure data aggregation scheme for WMSNs. Section 3 describes the proposed lightweight data aggregation scheme for WMSNs security based on similarity matching. Security analysis and performance evaluation are given in Section 4. Finally, Section 5 offers conclusions and future directions.

2. The Related Works

Sensor nodes in WMSNs have limited computing capability and energy resources without the aid of any established infrastructures, so many studies are conducted considering these limitations for various applications [5–11]. Multimedia data has a large volume which is different from traditional wireless sensor networks that transmit the simple numerical values, so important distinctions exist which greatly affects how security is achieved. Some of the related works in secure data aggregation are as follows.

Wu and Abouzeid [7] studied distributed image compression that the whole compression process of a single image was distributed among different groups of sensor nodes. The paper reduced the maximum energy needed in sensor nodes and did not decrease the total energy. Hongxia and Bangxu [8] 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. [9] presented a novel partial dynamic reconfiguration image sensor node prototype for WMSNs to transmit sensitive images. The paper enabled the partial dynamic reconfiguration to decrease the volume of image data. Czarlinska and Kundur [10] used back transmission to the cluster head when frames contain event of interest and studied the detection performance of event-driven WMSNs.

The scheme overcooked the hostile attacks using image processing techniques and supported a scalar sensor. Zhang et al. [11] focused on the design of transport protocols optimized for achieving fast transmission rates and fast error recovery, offering the application layer a better throughput of information which allowed using better resolution for the multimedia information. Ozdemir and Xiao [12] used integrity protecting hierarchical to conceal data aggregation for wireless sensor networks, but the volume of the multimedia data was not given significant consideration. Harjito et al. [13] provided a secure communication framework for WMSNs by developing new technique and developed a lightweight digital watermarking technique as a secure approach to ensure secure wireless communication. But the research did not describe the specific methods.

The existing schemes regarding sensor data aggregation for multimedia data sensors have just been studied from data transmission or energy efficiency. The volume of the multimedia data is not given significant consideration in some schemes, and even if some schemes have the advantages in energy efficiency or limited bandwidth, it has a security problem specifically. In short, evidence justifies that WMSNs security is indeed a very young research field, and the crucial question is how to prolong the resource-constrained WMSNs lifetime to the longest time in secured mode. We propose a secure data aggregation scheme based on similarity matching for multimedia data transmission to overcome bandwidth limitations and to solve the security problem.

3. The Proposed Scheme

In the paper, we describe a secure data aggregation scheme for multimedia data transmission. Firstly, we describe the similarity model and show how multimedia data is divided into some significant pieces data. Secondly, the process of the power model will be described in more detail.

3.1. The Similarity Model. In this section, we propose a method to provide the data aggregation for multimedia data (e.g., still image) transmission. To utilize the limited
Input: the standard piece data $x$
Output: the diverse divided piece $y$

Process:
(1) Initialization
(2) Compute the histogram normalization $M_s$ and $M_c$
(3) Compute the similarity specific value function $m$

$$m = M_s \cdot \log_2 \left( \frac{M_s}{M_c} \right)$$

(4) Compute the similarity matching function $S$

$$S = \begin{cases} 
S_{\text{high}}, & m < \varepsilon \\
S_{\text{low}}, & \text{other} 
\end{cases}$$

(5) Determine the similarity matching of $x$ and $y$, and choose the diverse divided piece $y$

**Algorithm 1: Image data similarity matching.**

---

**Figure 2: The similarity model.**

Considering the changes of surrounding, we capture one image data as the standard data once in a while and set other image data as the compared data. The proposed scheme splits the standard image data and the compared data into $n \times n$ pieces to achieve the similarity analysis, and piece $i$, piece $j$, and piece $k$ are the significant pieces because of the dissimilarity with the standard pieces. Each piece includes the coordinates and source node’s ID so that base station can conduct the reconfiguration for each packet. Compute the histogram normalization of the standard piece data and the compared piece data, respectively.

We define the similarity specific value function as

$$m = M_s \cdot \log_2 \left( \frac{M_s}{M_c} \right),$$

where $M_s$ is the value of the standard data normalization and $M_c$ is the value of the compared data normalization. We define the similarity matching function $S$ as

$$S = \begin{cases} 
S_{\text{high}}, & m < \varepsilon \\
S_{\text{low}}, & \text{other} 
\end{cases}$$

where $\varepsilon \in (m_{\text{min}}, m_{\text{max}})$. When $S = S_{\text{low}}$, we set the pieces data as reduplicate data and drop the packets.

When $S = S_{\text{high}}$, we transmit the pieces as the significant packets. As each divided piece of multimedia data is transmitted, even if any malicious node is tapping some packets, it is difficult to recover the original multimedia data. Moreover, if some packets are lost and the rest packets are received, the multimedia data also will be recomposed presumably.

In sum, the similarity matching algorithms are summarized in Algorithm 1.

According to the redundancy and similarity information of WMSNs surroundings, we compress the volume of multimedia data, decrease the data transmission, and enable sensor nodes to minimize the energy consumption of multimedia data transmission.

### 3.2 The Power Model

Data aggregation and data security are both indispensable aspects for WMSNs, but there is a significant risk of data aggregation. Under the model described above, we propose a similarity model to achieve the data aggregation. In the power model, we provide the data origin verification and authentication for secure data aggregation in WMSNs.
As sensor nodes are often deployed in noncontrolled environments, it will be possible for the attacker to access them and to imitate them. By compromising a node, the attacker may control all nodes actions [13]. The danger of data transmission requires data verification and authentication. Consequently, by legally adding an arbitrary number of malicious nodes and imitating good long-term behavior, all compromised nodes work together and transmit data. The major challenge for data verification and authentication is to exactly know which sensor nodes are malicious in WMSNs. The power model uses multimedia data regular statistic approach to define the rules within the fuzzy system. Three power values are defined as $H_0$ (low power), $H_1$ (medium power), and $H_2$ (high power). The power values reflect a node’s operation state and whether or not other nodes want the node to be available as a resource for cluster jobs. The concept of the power model is shown in Figure 3.

Specifically when the power value is $H_0$, we describe the sensor node as malicious node, and then this state indicates that the node was rejected by a cluster administrator and other sensors. The power value $H_2$ is held by the normal node, and this state indicates that the node accept and run any cluster jobs. Similarly, $H_1$ means the sensor node in a pending state. In our work, we initialize the power value of every node as $H_2$ state. We regard the captured multimedia data as the standard data at a set time, split the standard data in $n \times n$ pieces, and record the statistical regularities of each piece. The crucial step is to record the numbers of pieces in the $n \times n$ pieces which contain the similarity specific value $m$ greater than $\varepsilon$. When number of values is greater than a threshold, we update the state as $H_0$ or $H_1$. In particular, $H_0$ state indicates that the node is malicious, and sensor nodes of the power value $H_1$ keep waiting for the next determination when the standard data are captured again.

Under the power model described above, we utilize three power values to identify the valid nodes, so as to enhance
the security of data aggregation and provide the data origin verification and authentication for multimedia data.

4. Performance Analysis and Result

4.1. Experiment Configuration. In this section, we perform extensive simulations to measure the performance of our proposed scheme and validate the analytical results. In order to evaluate the effectiveness of our proposed algorithm, we first compare our proposed scheme with the scheme without processing and the distributed image compression scheme proposed in [7] with respect to the total transmission volume as well as the energy consumption of each sensor node when the sensor nodes transmit the multimedia data on single hop networks. Considering the security verification, we describe the malicious node detection rate and the false alarm rate with the variation of the malicious nodes proportion. Balancing image quality and energy consumption, the image quality is measured by the mean square error (MSE).

We run the simulation on each generated input file for target tracking scenarios with each of the parameters described in Table 1.

In order to evaluate our approach in a simulated scenario, the wireless sensor network simulator is implemented in MATLAB. Assume that 50, 100, and 150 sensors are, respectively, deployed uniformly in a 100 × 100 (m) network field and the radius of communication is 25 m. Each node has randomized x and y coordinates. No two different nodes share the same coordinates. The spatial resolution of the still images data is all 256 × 256, and we present results with ε = 0.625 and n = 8.

4.2. Experiment Analysis and Result. In this section, Figure 4 demonstrates the results in terms of the total transmission volume in different numbers of sensor nodes. With the numbers of sensor nodes growing, the total transmission increases. Obviously, the proposed scheme provides a less transmission volume than the existing schemes and the scheme without processing. From the result of simulation analysis, the amount of transmission volume is reduced by about 20%.

Sensor nodes of various functionalities have been put into use, and then the energy consumed by different sensor nodes are disparate during different operations. For comparison purposes, the paper supposes that 50 sensors on single hop networks transfer the multimedia data in order. As shown in Figure 5, the 1st node consumes about 800 mA energy while the average consumption of other nodes is 210 mA. The energy consumption of the 1st node consumes is more than twice times that of other nodes. But the proposed scheme decreases the total energy consumption and reduces the total transmission volume in wireless multimedia sensor networks. The comparison empirically shows that our proposed method is efficient and can achieve results that compare favorably with the existing methods.

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 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. The result achieves a low false alarm rate.

Considering the complexity of the image data, we group scenarios into three different types: simple, general, and complex. Figure 8 shows the overall MSE of the whole reconstructed still image from various scenarios. The overall MSE is the average value of the MSEs of each block of data. It can be observed that the image qualities of our proposed scheme, exiting scheme, and without processing have some errors introduced in the process of similarity model during the data aggregation at intermediate nodes. Along with the scene complexity increases, the proposed scheme makes more obvious immediate advantage.

5. Conclusions

Wireless multimedia sensor networks will become ubiquitous in our daily life and they have already been a hot research...
area for the past couple of years. In order to improve the performance of the multimedia transmissions in WMSNs, we propose a novel secure data aggregation algorithm by making use of certain knowledge about the characteristics of the transmitted multimedia information. We define a similarity specific value function and describe the similarity model according to the redundancy information of WMSNs surroundings, which enable sensor nodes to minimize the energy consumption of data transmission. Then, with the similarity surroundings, we develop the power model to provide data verification and authentication for security in WMSNs. Through performance evaluation, the proposed scheme has shown that the amount of energy consumption is reduced by about 20% and data origin verification and authentication provides the basis security in an aggregating sensor network. Finally, we show the overall MSE of the whole reconstructed still image from various scenarios. Along with the scene complexity increases, the proposed scheme makes more obvious immediate advantage. As a result, the scheme can be applied to provide optimal secure data aggregation and ensure minimum energy consumption. In future work, we plan to take multimedia data encryption into account and further improve similarity matching performance.

**Conflict of Interests**

The authors declare that they do not have any commercial or associative interest that represents 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 no. 110818001 and Grant no. 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, T. Melodia, and K. R. Chowdhury, “A survey on wireless multimedia sensor networks,” *Computer Networks*, vol. 51, no. 4, pp. 921–960, 2007.

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

[3] C. S. Deshmukh and S. V. Dhopate, “Network environment using compressed 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.

[4] X. L. Sun, X. G. Sun, and S. S. Li, “The key management scheme for the WMSN-based post-disaster road monitoring system,” *Advanced Materials Research*, vol. 756–759, pp. 332–337, 2013.

[5] D. Kim, G. Cagalaban, and M. Kim, “Efficient data aggregation scheme for wireless multimedia sensor networks,” *Journal of Security Engineering*, vol. 10, no. 3, 2013.

[6] S. Pudlewski, T. Melodia, and A. Prasanna, "C-DMRC: compressive distortion-minimizing rate control for wireless multimedia sensor networks," in *Proceedings of the 7th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON’10)*, Boston, Mass, USA, June 2010.

[7] H. Wu and A. A. Abouzeid, “Energy efficient distributed JPEG2000 image compression in multihop wireless networks,” in *Proceedings of the 4th Workshop on Applications and Services in Wireless Networks (ASWN ’04)*, pp. 152–160, August 2004.

[8] W. Hongxia and Y. Bangxu, “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.

[9] 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.

[10] A. Czarlinska and D. Kundur, “Reliable event-detection in wireless visual sensor networks through scalar collaboration and game-theoretic consideration,” *IEEE Transactions on Multimedia*, vol. 10, no. 5, pp. 675–690, 2008.

[11] L. Zhang, M. Hauswirth, L. Shu, Z. Zhou, V. Reynolds, and G. Han, “Multi-priority multi-path selection for video streaming in wireless multimedia sensor networks,” in *Ubiquitous Intelligence and Computing*, vol. 5061 of *Lecture Notes in Computer Science*, pp. 439–452, Springer, Berlin, Germany, 2008.

[12] S. Ozdemir and Y. Xiao, “Integrity protecting hierarchical concealed data aggregation for wireless sensor networks,” *Computer Networks*, vol. 55, no. 8, pp. 1735–1746, 2011.

[13] B. Harjito, S. Han, V. Potdar, E. Chang, and M. Xie, “Secure communication in wireless multimedia sensor networks using watermarking,” in *Proceedings of the 4th IEEE International Conference on Digital Ecosystems and Technologies (DEST ’10)*, pp. 640–645, Dubai, United Arab Emirates, April 2010.
