Cooperative Data Deployment Scheme for Better Context Inference in Wide Area Surveillance Environment

Soomi Yang and Pil Seong Park

***Abstract*—In an intelligent decentralized wide area surveillance environments which cooperate with each other, efficient data deployment strategy is needed for agile integrated reasoning. An overwhelming amount of multimedia data with event data and feature data is generated continuously by surveillance devices such as smart cameras or various sensors. Surveillance data contained in them if they are interoperable, properly be structured and integrated, can induce useful context information. This paper builds a hierarchical surveillance data deploy structure and import related data from others to annotate data arriving from multiple data source devices. The annotation process provides an impetus to the improvement of knowledge over time. Proactive surveillance data deploying provides the main concepts and properties to model a hierarchical area data structure. We define management policies helping agent's reasoning process, discuss the design and implementation details of this network and compare their performance for the wide area surveillance.**

***Index Terms*—Data deployment strategy, Wide area surveillance system, Cooperative reasoning, Multimedia data management.**

I. Introduction

For the surveillance of the large area, agents built in networked RFID sensors, CCTVs and smart cameras explore the convergence of the data deploying and streaming technologies for multimedia data to collaborate through integration of other data such as device profile data, event data, biometric data and feature data. Especially, smart cameras are embedded systems that can perform on-board input analysis and report surveillance data resulted to other smart cameras or other varible surveillance components. We use the term surveillance data to include audio, video, recognized feature data, ontology data and others. Most surveillance data transfers take place with the streaming data passing through one or more of the agents. The collected information, if properly structured, provides an overview of the activity in large area and helping making an sagacious decision as reaction. Effective data deploy techniques will be critical for the successful deploy of heavy streaming multimedia data over the surveillance network.

This paper describes a framework for the working of such a distributed data deploying and management system. Distributed agents receiving heterogeneous data from various sources have autonomy, collaborate with each other, and do ontology reasoning based on distributed knowledge bases.

In the process of reasoning each agent may process the consolidated data for the distributed and autonomous reasoning, which is scalable and efficient[1], helps security persons by giving appropriate decision or prediction based on huge ontology data about situation it gathers.

The rest of the paper is organized as follows, Section 2 surveys related work of cooperative inference schemes. Section 3 describes the adaptive surveillance data management technique. In Section 4, implementation results are presented and the performance is evaluated. Finally, Section 5 concludes.

Manuscript received October 9, 2001; revised April 5, 2012. (Write the date on which you submitted your paper for review.) This work was supported in part by the U.S. Department of Commerce under Grant BS123456 (sponsor and financial support acknowledgment goes here). Paper titles should be written in uppercase and lowercase letters, not all uppercase. Avoid writing long formulas with subscripts in the title; short formulas that identify the elements are fine (e.g., "Nd–Fe–B"). Do not write "(Invited)" in the title. Full names of authors are preferred in the author field, but are not required. Put a space between authors' initials.

Soomi Yang is with the Department of Information Security, the University of Suwon, Hwasungsi, 445-743 KOREA (e-mail: smyang@suwon.ac.kr).

Pil Seong Park is with the Department of Computer Science, the University of Suwon, Hwasungsi, 445-743 KOREA (e-mail: pspark@suwon.ac.kr).

II. Related Work

Numerous studies have been carried out on the data management techniques in distributed environments. For a wide area physical security surveillance, monitoring systems are connected to communicate with each other [2, 3, 4, 5]. Especially [6, 7] dealt with multimedia data which is the most interested data format for the surveillance environment. However, previous works were mostly based on the ground that the distributed nodes in the network have the same characteristics, and the data transmitted is standardized and intermittent. Our distributed surveillance environment consisted of various data source devices, multimedia data is generated continuously and analysis should be done in real time.

To increase interoperability and ease merging of heterogeneous data, effort for the standardization for physical security is done by ONVIF (Open Network Video Interface Forum) [8] and PSIA (Physical Security Interoperability Alliance) [9]. They define, recommend, and promote standards for IP-based security products. Besides ISO [10], BSI group [11], other standard organizations enact standards for general aspect of physical security. Our implemented system tried to meet the requirements of industry by providing functions recommended by standard organizations. [12] also builds decentralized wide area surveillance networks based on ONVIF. They displayed information collected in a 3D model of the surveilled data, therefore provideing a comfortable overview of the activity

in large environments and offering the user an intuitive way to interact with network devices. However they do not integrate data analysis with reasoning engine and do not provide management scheme of large surveillance data.

Many of existed security surveillance system depend on the knowledge annotated by experts[13, 14]. There are few of surveillance systems adopting ontology-driven technologies[7, 15]. [16] introduces artificial intelligence techniques only for the interpretation of objects. [17] uses ontology but does not build agents for web of data. Furthermore existing wide area surveillance system are closed system and do not provide scalability based on efficient data deployment.

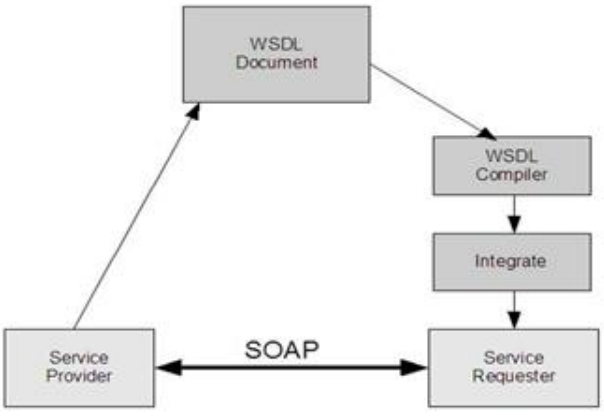
For a decentralized surveillance networks management, [18] introduces distributed tracking system using ontology for cooperation. [19] suggests network buffer management which can be generally used , but is not specialized for surveillance networks. [20] has dealt with object detection, tracking and recognition for multiple smart cameras in small area. Many of wide area surveillance networks are closed system and do not provide surveillance information as a public web services which is suggested in the standard. We try to meet the standard and accomplish efficient surveillance data management.

III. Cooperative Surveillance Data Management

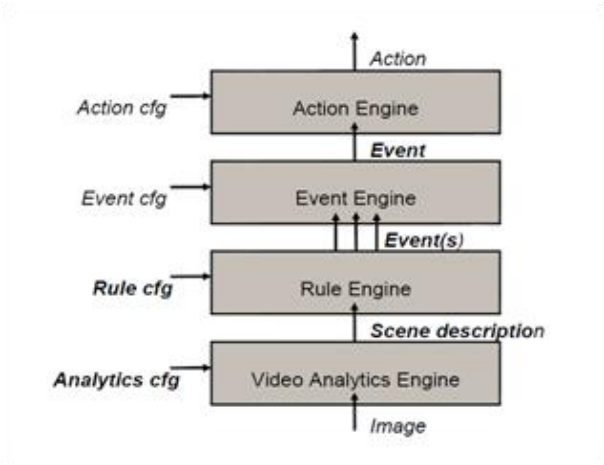
A. System Framework

Our framework architecture consists of a hierarchy of agents, which contains a number of non-leaf node administrative agents and leaf node agents with sensors. It consists of national agents at the top, some regional agents at the middle level, and many local agents at the second lowest level. At the lowest level, data source agents such as agents built in smart camera make leaf nodes.

The servers can communicate each other freely within access control permission to perform their own intelligent distributed context inference based on their own ontology knowledge base integrated with imported ontology data. Agents in each server is built and communicate each other following the ONVIF standard as seen in Fig. 1.



(a) Web Services based deve lopment pr inciples



(b) Video analytics architecture

Fig. 1. Standard web service configuration recommended in ONVIF [8]

In our wide area surveillance environment, every agent possibly built in smart camera provides web services as defined in ONVIF standard. Web services are standardized method of integrating applications using open, platform independent based on standards such as XML[21], SOAP[21], WSDL[21] over an IP network.

Fig. 1(a) gives an overview of the basic principles for development based on web services. The service provider, agent in our system, implements the ONVIF services. The service is described using the XML-based WSDL given in ONVIF specifications. The WSDL is used as the bases for the service requester, agent related to administrator in our system, implementation. Service requester-side implementation should be done through the use of WSDL compiler tools that generate stub code that can be used by the requester side developer to integrate the web service into an application.

The web service provider and requester communicate using the SOAP message exchange protocol. Although SOAP is heavier than general RPC(Remote Procedure Call), it is rich and easy to use.

Fig. 1(b) is shows video analytics architecture from image to action. Our inference engine adopts this framework which enables a client to contact a device implementing the ONVIF for supported analytics modules and the configurations.

Deploying data in surveillance network has usually a hierarchical architecture on top of the hierarchical administration organization. These data, often referred to as institutional, regional, and national data depending on the hierarchy of the administrative agents operating them, is integrated with each other so as to infer and deliver efficiently the requested result to the users. For distributed data, even small agents, with the help of higher level agents, can achieve very high hit rate locally, thus reducing significantly the bandwidth requirements of the network connection and the latency perceived by the users.

Our system framework assumes a proactive, rather than reactive, deploying of data. By proactive deploying, it means that the middle level agents cooperate with the master in exchanging necessary information on the data size, the request rate and so on, enabling the master to fetch and broadcast the data before a lower level agents requests it. To achieve this goal, the surveillance network is modeled as a multi-layered distribution network. The system performances

like hit rate, disk space, bandwidth gain of the agents and the leaf node source servers, bandwidth for the surveillance network, and latency experienced by the users are derived.

For our experiment, single server with CCTV is constructed as seen in Fig. 2. It emulates ONVIF smart camera as a testbed. We observe and modify the experiment steps and measure the performance metric.

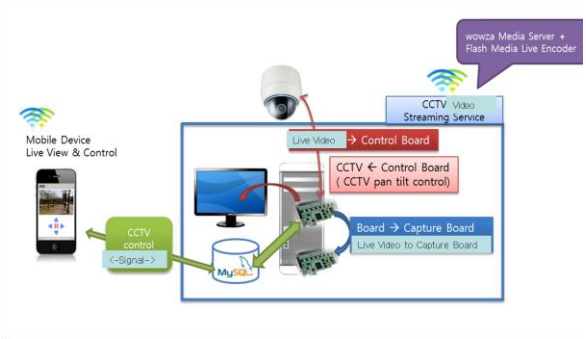


Fig. 2. Single site constitution with CCTV

B. Data Deployment Scheme Analysis

For the performance analysis, we specify some features of the forwarding data in multi-layered network. We define $D=\{1,2,\ldots,|D|\}$ as the whole set of data, and assume that the data in D are ranked in the order of their suspiciousness or importance. From the well-known results that the probability of the i-th data is Zipf distributed, we have the related probability function [6, 22].

To maintain the freshness and effectiveness of the data, we should manage data adaptively. We use the term 'weight' of data to describe its relative importance as compared to the other data as proposed in [23]. The higher the weight, the lower is the probability of the clip being replaced. We also use a policy based on the size of the objects, in which the weight is proportional to the inverse of the size of the data for the network bandwidth usage efficiency. Therefore the weight w is computed as following, where F is the number of times the data is accessed, S is the size of the data and R is the time since the last access for the data. The three exponents f, r and s are weighting factor. Every agent operates the same set of data for some designated suspect, the expression for δ_k being the same and independent to the other connected agent k.

$$\begin{aligned} w &= F^f S^s R^r \\ &= \lambda_{ki}{}^f \delta_k{}^s \mu_i{}^r \\ &= (\beta n_k \cdot \frac{\sigma}{i^\alpha})^f \cdot (\sum_{i \in D_F} S_i)^s \cdot \mu_i^r \end{aligned} \quad (1)$$

where μ_i is the update interval. The value for f should be a positive number, meaning that more frequently accessed data is more likely to be found. The value of s can be should be a negative number for the efficient use of network bandwidth, such that more small data is more likely to be stored. The value of r should be a negative number, meaning that more recent data is more likely to be stored. If the recentness is more important than the frequency, the absolute value of the exponent r should be greater than that of the exponent f.

With the same preference distributions and the same set of data, all the subscribing agents have the same hit rate as a distributed surveillance environment and multimedia data and feature data are produced continuously. If we let the probability of data miss according to a Poisson process with the same rate to keep the number of data miss in the system roughly constant, the probability of having data miss at each server, P can be computed as the following Equation (2).

$$P = 1-(1-e^{-\mu T})\cdot\frac{1}{\mu T} \quad (2)$$

$(1-e^{-\mu T})$ is the cdf(cumulative distribution function) of an exponential distribution. T is the maximum time it takes to detect the data miss. We can reduce the data miss probability P, with proactive data deploying according to the previously calculated w.

IV. Performance Evaluation

A. Simulation

For the performance evaluation, the data miss rate is calculated according to the following Equation (3).

$$Q = (f(P) - f(w))/f(P) \quad (3)$$

where $f(P)$ is the amount of the data miss according to the Equation (5) and $f(w)$ is the amount of the prefetched data based on the Equation (2). The data miss rate diversity with the data update interval and the weight threshold is shown in Fig. 3. Because other factors such as data rank, size, etc., there are many surplus values plotted in the graph. In the figure, we show values in regard to the data update interval μ_i.

Our cooperative and proactive data deployment strategy shows more performance gain for the short update interval. For the adaptive deploying technique, we can raise the weight threshold value for the proactive caching. When we increase the threshold value, the data miss rate Q decreases resulting in better data integration for cooperative reasoning.

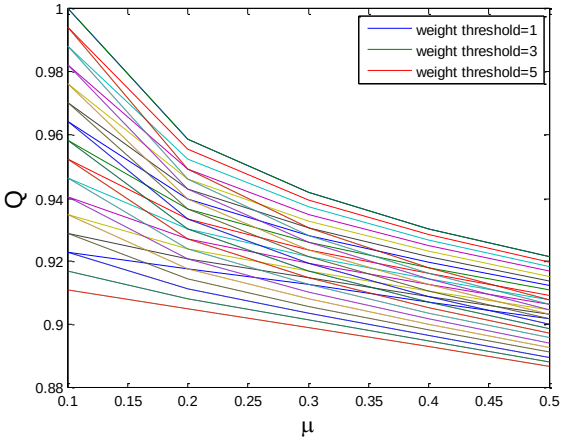


Fig. 3. The data miss rate diversity with the data update interval and the weight threshold

B. Implementation

We implemented our cooperative data deploy framework for integrating surveillance data with an adaptive deploying technique presented in this paper into our distributed surveillance system.

Fig. 4 shows several screenshots of user interfaces. In Fig.

4 (a), it shows a web interface with Google map. On the top left side of the screen, the user can see the list of surveillance servers in its domain. By clicking specific camera name, live video from designated camera server can be seen as shown in the popup window. On the bottom left side of the screen, the user can choose other surveillance area under the user access control. On the top right side of the screen, the user can see the list of alarming locations. By clicking some specific alarm, stored video or the real-time view of the site can be seen depend on the characteristics of the event. At the middle on the right side frame, we can see the legend for the markers. On the bottom right side of the screen, stored video can be searched through typed keywords

In Fig. 4(b), it shows a mobile interface with Google map and control plane. They should be switched for small screen panel. More functions are under developing. Our system is going to provide a highly customizable graphical user interface for specifying user-defined policies

The subject tracking through the communication between the independent agent which is monitored through different user interfaces, is possible as shown in Fig. 4. They inquire feature data for a combined inference through defined queries which are conformed to standard and receive related trace information.

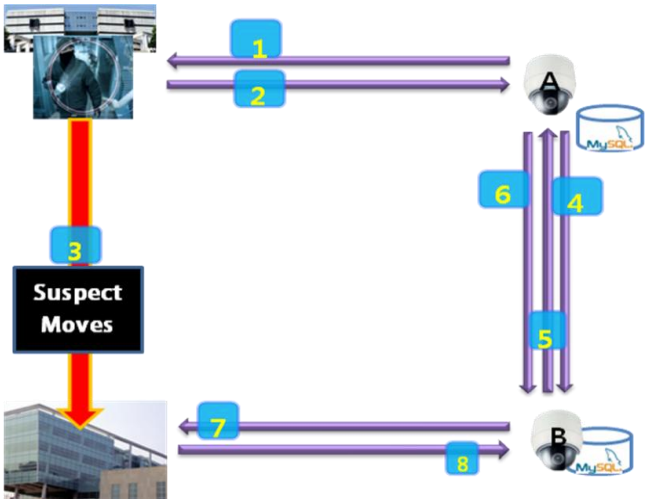
(a) Web interface with Google map

(b) Mobile interface with Google Map and camera control plane

Fig. 4. Subject tracking between several smart cameras

C. Subject Tracking Scenario

Most detection and tracking systems that have been developed or proposed collect information from multiple cameras at a central point in the network. Analysis and decision making are centralized. It is responsible for establishing tracks and associating measurements from different views. As the number of cameras grows, increasing demands are placed on the communication system which must route information to central system. In order to get around this problem, we develop approaches to detect and track subject which can be distributed over multiple cameras without requiring excessive amounts of communication. It must be scalable to allow for deployments that may involve thousands of cameras distributed over extended regions and must be robust to failure so that the overall system responds gracefully when individual cameras are added or removed asynchronously. The summarized scenario which only contains the key points of cooperation between the cameras is shown in Fig. 5.



(a) Conceptual diagram for tracking

1: Broadcast Search request increasing TTL(Time to Live) for features of suspect if there is no cached information.
2: Reply current location with the inference result about the trace of suspect.
3: Suspect moves.
4: Send trace command to candidate destination cameras based on the inference result integrated.
5: Confirm appearance of suspect and request trace information.
6: Reply information about location, features of suspect for trace.
7: Verify the information about the suspect and infer the future scenario and make a decision as reaction.
8: Update trace information based on the new Surveillance data obtained and send resulted data to cameras related.

(b) Summarized procedure

Fig. 5. Subject tracking scenario

V. Conclusion

In this paper, we propose a flexible cooperative surveillance data deploying scheme which is adaptive to the actual device demands and that of its neighbors. We designed a large-scale surveillance system framework which complies

with the ONVIF specification. The ONVIF specification defines a protocol for the exchange of information between surveillance devices providing seamless interoperability. We use conformity to update and share data in a cooperative way on the standard framework. The specification includes device discovery, video streaming, metadata and use of web services to efficiently provide interoperability between devices. It helps better cooperative inference performed at each agent in wide area surveillance.

The system we implemented is composed of smart cameras and RFID sensors whose captured video sequences are analyzed in its agent and exchange information with the neighbor agents. As a user interface, we implemented web interface and mobile interface. They provide comprehensive views of the monitored environment and offer the user an intuitive way to interact with surveillance devices.

Our project is aimed to cover Gyeonggi province which contains over 30 cities. We build test bed in the university and apply our data management scheme. Implementation is going on to be installed in Gyeonggi province decentralized surveillance network environment.

Simulation studies are conducted to evaluate the effectiveness of our flexible surveillance data deploying scheme. Based on mathematical derivations, the proactive deployment of surveillance data maximizes the reasoning engine's potential for making decisions from operating the hierarchical structure distribution. Computational experiments investigate how the optimal deployment scheme and service policy responds to system parameter changes. It shows the efficiency of surveillance data deploying resulted in better integrated context inference.

ACKNOWLEDGMENT

Soomi Yang and Pil Seong Park thank to Jong Yeol Lee, Jae Wook Oh and Jeong Hwi Kim for their help and comments across project years.

This work is supported by the GRRC program of Gyeonggi province. [GGA0801-45700, Center for U-city Security and Surveillance Technology, GRRC SUWON2011-B1].

REFERENCES

[1] A. Schlicht and H. Stuckenschmidt, "Towards Distributed Ontology Reasoning for the Web," WI-IAT08, 2008, pp. 536-539.
[2] K. Kozaki, E.Sunagawa, Y. Kitamura, and R. Mizoguchi, "A Framework for Co-operative Ontology Construction Based on Dependency Management of Modules," *Proceedings of the Workshop on Emergent Semantics and Ontology Evolution*, 2007, pp. 33-44.
[3] D. Lymberopoulos, T. Teixeira, and A. Savvides, "Macroscopic Human Behavior Interpretation Using Distributed Imager and Other Sensors," *Proceedings of the IEEE*, vol. 96, no. 10, 2008, pp. 1657-1677.
[4] N. Siebel and S. Mybank, The Advisor Visual Surveillance System, "Applications of Computer Vision," 2004, pp. 103-111.
[5] M. Shah, O. javed, and K. Shafique, "Automated visual surveillance in realistic scenarios," *IEEE Multimedia*, vol. 14, no. 1, 2007, pp.30-39.
[6] T R Gopalakrishnan Nair and P Jayarekha, "A Rank Based Replacement Policy for Multimedia Server Cache Using Zipf-Like Law," *Journal of Computing*, vol. 2, Issue 3, 2010.
[7] J. Z. Pan, "A Flexible Ontology Reasoning Architecture for the Semantic Web," *IEEE TKDE*, vol. 19, no. 2, 2007.
[8] ONVIF (Open Network Video Interface Forum) http://www.onvif.org
[9] PSIA Specification Package Q12009, http://www.psiaalliance.org
[10] http://www.iso.org
[11] http://www.bsigroup.com
[12] T. Senst, M. Patzold, R. H. Evangelio, V. Eiselein, I. Keller, and T. Sikora, "On Building Decentralized Wide-Area networks based on ONVIF," *IEEE Workshop on Multimedia Systems for Surveillance(MMSS)* , 2011, pp. 420-423.
[13] N. Kodali, C. Farkas, and D. Wijesekera, "Enforcing Semantics-Aware Security in Multimedia Surveillance," *Journal on Data Semantics II*, 2005, pp. 199-221.
[14] R. Piltaver and G. Matjaz. "Expert system as a part of intelligent surveillance system," *Proceedings of the 18th International Electrotechnical and Computer Science Conference—ERK*, 2009, vol. B, 2009, pp. 191-194.
[15] Chulki Lee, Sungchan Park, Dongjoo Lee, Jae-won Lee, Ok-Ran Jeong, and Sang-goo Lee, "A Comparison of Ontology Reasoning Systems Using Query Sequences," *Proceedings of The Second International Conference on Ubiquitous Information Management and Communication*, 2008, pp. 560-563.
[16] R. Martinez-Tomas, M. Rincon, M. Bachiller, and J. Mira, "on the correspondence between objects and events for the diagnosis of situations in visual surveillance tasks," *Pattern Recognition Letters*, vol. 29, Issue 8, 2008, pp. 1117-1135.
[17] Roberto Vezzani and Rita Cucchiara, ViSOR: "Video Surveillance On-line Repository for annotation retrieval," *IEEE International Conference on Multimedia and Expo*, 2008, pp.1281-1284.
[18] J. Gomez-Romero, M. A. Patricio, J. Garcia, and J. M. Molina, "Communication in distributed tracking system: an ontology-based approach to improve cooperation," *Expert Systems (The Journal of Knowledge Engineering)*, vol. 28, no. 4, pp. 288-305, 2011.
[19] K. Chitra and Dr. G. Padmavathi, "FAVQCHOKE: To Allocate Fair Buffer to a Dynamically Varying Traffic in an IP Network," *International Journal of Distributed and Parallel Systems (IJDPS)* Vol.2, No.1, pp.73-81, 2011.
[20] A. Sankaranarayanan, A. Veeraraghavan, and R. Chellappa, "object Detection, Tracking and Recognition for Multiple Smart Camaras," *Proceedings of the IEEE*, vol. 96, no. 10, 2008, pp. 1606-1624.
[21] http://www.w3.org.
[22] L. Adamic and B. Huberman, "Zipf's law and the Internet," *Glottometrics*, vol. 3, 2002, pp. 143-150.
[23] A. Paknikar, M. Kankanhalli, and K. Ramakrishnan, "A Caching and Streaming Framework for Multimedia," *ACM Multimedia*, 2000.

(All authors should include biographies with photo at the end of regular papers.)

Soomi Yang received the B.S., M.S. and Ph.D. degrees in computer engineering from Seoul National University of Seoul, Korea, in 1985, 1987 and 1997 respectively. From 1988 to 2000, she was a researcher at Korea Telecom Research Center where she worked on telecommunication network, internet and information security. From 2000 to 2001, she was a visiting scholar at UCLA, USA. From 2002 to 2004, she was a faculty of the Suwon Science College, Korea. Since 2004, she has been on the Faculty of the University of Suwon, Korea, where she is a professor of computer science. Her research interests in information security include access control, network security, and secure system software.

Pil Seong Park received the B.S. degree in Physical Oceanography from Seoul National University, Korea in 1977, and the M.S. degree in Applied Mathematics from Old Dominion University, U.S.A. in 1984. He received the Ph.D. degree in Interdisciplinary Applied Mathematics (with emphasis on computer science) from University of Maryland at College Park, U.S.A in 1991. He worked as the head of Computer Center at Korea Ocean Research ang Development Institute from 1991 to 1995. Currently, he is a professor of the Department of Computer Science, University of Suwon in Korea. His research interest includes high performance computing, Linux clusters, digital image processing, and knowledge-based information systems. He is a member of several academic societies in Korea.