Advances in Multimedia

Advanced Issues on Topic Detection, Tracking, and Trend Analysis for Social Multimedia

Guest Editors: Seungmin Rho, Wenny Rahayu, and Uyen Trang Nguyen

Advanced Issues on Topic Detection, Tracking, and Trend Analysis for Social Multimedia

Advances in Multimedia

Advanced Issues on Topic Detection, Tracking, and Trend Analysis for Social Multimedia

Guest Editors: Seungmin Rho, Wenny Rahayu,
and Uyen Trang Nguyen

Copyright © 2015 Hindawi Publishing Corporation. All rights reserved.

This is a special issue published in "Advances in Multimedia." All articles are open access articles distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Editorial Board

Ehab Al-Shaer, USA
Marios C. Angelides, UK
Luigi Atzori, Italy
Noboru Babaguchi, Japan
Bharat Bhargava, USA
Patrizio Campisi, Italy
R. Chandramouli, USA
Shu-Ching Chen, USA
Liang T. Chia, Singapore
Juan C. De Martin, Italy
David H. Du, USA
Jianping Fan, USA
George Ghinea, Norway
William I. Grosky, USA
Pengwei Hao, UK
Xian-Sheng Hua, China
H. Jiang, Canada
Jesse S. Jin, Australia
Hari Kalva, USA
Darko Kirovski, USA
Stefanos Kollias, Greece
C. Kotropoulos, Greece
Qingshan Liu, China
Alexander Loui, USA
Tao Mei, China
Chong Wah Ngo, Hong Kong
B. Prabhakaran, USA
Thierry Pun, Switzerland
Deepu Rajan, Singapore
Martin Reisslein, USA
Marco Roccetti, Italy
G. (Jacky) Shen, China
Timothy K. Shih, Taiwan
Mei-Ling Shyu, USA
Jaideep Srivastava, USA
Po-Chyi Su, Taiwan
Yap-Peng Tan, Singapore
Da Cheng Tao, Singapore
Qi Tian, Singapore
Deepak Turaga, USA
T. Turletti, France
D. Tzovaras, Greece
Andreas Uhl, Austria
A. V. Vasilakos, Greece
Jianfeng Wang, USA
Jianfeng Wang, USA
Shiqiang Yang, China
H. Yin, China
Zhongfei Zhang, USA
Chengcui Zhang, USA
Jiying Zhao, Canada

Contents

Hindawi Publishing Corporation
Advances in Multimedia
Volume 2015, Article ID 709646, 2 pages
http://dx.doi.org/10.1155/2015/709646

Editorial

Advanced Issues on Topic Detection, Tracking, and Trend Analysis for Social Multimedia

Seungmin Rho,[1] Wenny Rahayu,[2] and Uyen Trang Nguyen[3]

[1]*Department of Multimedia, Sungkyul University, Anyang-si, Gyeonggi-do 430-742, Republic of Korea*
[2]*Department of Computer Science and Computer Engineering, La Trobe University, Bundoora, VIC 3086, Australia*
[3]*Department of Computer Science and Engineering, York University, Toronto, ON, Canada M3J 1P3*

Correspondence should be addressed to Seungmin Rho; pc.seungminrho@gmail.com

Received 16 March 2015; Accepted 16 March 2015

Copyright © 2015 Seungmin Rho et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Introduction. In recent years, the smartphone boom has made social media monitoring of news, blogs, Twitter, and Facebook a social phenomenon. Twitter is an online social networking and microblogging service that has gained worldwide popularity with over 500 million active users as of 2012. Even though one tweet may contain at most 140 characters, the number of tweets that are generated daily is enormous and hence they, collectively, could give important clues to several issues such as public opinions, current trends, and burst keywords. If detecting the information could be successfully done, various services related to the information, such as multimedia contents recommendation and trend contents visualization, can be provided. So far, many studies have been carried out for this goal. Therefore, we are looking for efficient and effective meaningful information such as topic and trend detecting/tracking algorithms in SNS (social network services) big data.

Each submitted manuscript was blindly reviewed by at least three reviewers consisting of guest editors and external reviewers. After two review processes, nine manuscripts were selected to be included in this special issue. In Summaries of Selected Manuscripts, we briefly summarize these manuscripts.

Summaries of Selected Manuscripts. The article entitled "Study on Strengthening Plan of Safety Network CCTV Monitoring by Steganography and User Authentication" by J. O. Park and S. Kim proposes an image checking technique through steganography to ensure the security of the image transfer process and user authentication protocol to block malicious users in network CCTV environments.

In the paper entitled "Supporting Image Search with Tag Clouds: A Preliminary Approach," F. Guerra et al. introduce a novel tag-based system supporting the search of images published with some textual information. For two particular use cases, they also implement *MediaPresenter* which is a system for (i) the creation of multimedia presentations and (ii) an image search engine for Twitter.

In the paper entitled "Performance Comparison of OpenMP, MPI, and MapReduce in Practical Problems," S. J. Kang et al. review existing parallel computing models and present performance studies of three widely recognized parallel programming frameworks: OpenMP, MPI, and MapReduce. The comparative study was conducted for two problem sets: the all-pair shortest path problem and a joint problem for large data sets.

The paper entitled "Security Requirements for Multimedia Archives" by S. B. Park presents security issues related to digital archive systems. The author discusses security problems of cryptographic primitives and lifetime of cryptographic keys for long term preservation. For long term security, the author suggests periodic updates of cryptographic messages and keys. The study is not to solve those problems but rather to enumerate the requirements which must be considered for secure digital archiving systems.

In the paper entitled "Coevolution of Artificial Agents using Evolutionary Computation in Bargaining Game," S. Lee investigates the interaction and coevolutionary process

among heterogeneous artificial agents using evolutionary computation (EC) in the bargaining game. The three kinds of EC based agents are compared in the bargaining game: genetic algorithm, particle swarm optimization, and differential evolution. The game performance with regard to payoff through the interaction and coevolution of agents is studied. The study demonstrates that the particle swarm optimization approach is superior to the other algorithms in the bargaining game.

In the paper entitled "Preprocessing Techniques for High-Efficiency Data Compression in Wireless Multimedia Sensor Networks," J. Park and J. Yoo propose novel preprocessing techniques for high-efficiency data compression in wireless multimedia sensor networks. The proposed techniques consider the characteristics of sensed multimedia data to perform the first stage preprocessing by deleting the low priority bits that do not affect the image quality. The second stage preprocessing is also performed for the undeleted high priority bits. These preprocessing techniques significantly reduce the size of multimedia data to be compressed. To show the superiority of the proposed techniques, an existing multimedia data compression scheme with and without our preprocessing techniques was implemented. The experimental results have shown that the proposed techniques increase the compression ratio while reducing the number of compression operations compared to the existing compression scheme without the preprocessing techniques.

The paper entitled "Discovering Congested Routes Using Vehicle Trajectories in Road Networks" by K. S. Bok et al. proposes a new discovering scheme of congested routes through the analysis of vehicle trajectories in a road network. The proposed scheme computes the complexity value of each road segment according to different directions and detects congested routes of a road network by clustering congested road segments within each time interval. To show the superiority of the proposed scheme, a performance evaluation was performed by comparing the proposed scheme with the existing scheme NETSCAN. The experimental results show that the proposed scheme can efficiently discover congested routes in different directions better than the existing scheme.

In the paper entitled "An Empirical Analysis of Technology Transfer of National R&D Projects in South Korea," M.-S. Kim et al. examine the outcomes of national R&D projects by the types of R&D organizations and by the types of R&D and analyze the factors influencing the outcomes. Their analysis indicates that there were significant differences between government funded institutions and universities and between basic and applied R&D. The study has found that government funded institutions did not necessarily perform better than universities in terms of the quantity of technology transfer.

In the paper entitled "Development of Ontology and 3D Software for the Diseases of Spine," S. Lee et al. introduce an e-Spine project carried out by the Korea Institute of Science and Technology Information (KISTI) that deals with spinal diseases to prepare for an ageing society. They built an ontology of the spine with links to the causes, symptoms, and methods of treatment of frequently encountered spinal diseases among Koreans and anatomical information. The completed spinal ontology expresses anatomical connections of the parts of the spine and their vertical relationships as well as information on spinal diseases. It is easy to understand the spinal structure and diseases by conceptualizing the anatomical structure of the spine and showing it in 3D images.

Acknowledgments

Our special thanks go to the editorial board members of this journal for their valuable supports throughout the preparation and publication of this special issue. We would like to thank all authors for their contributions to this special issue. We also extend our thanks to the external reviewers for their time and efforts in reviewing the manuscripts.

Seungmin Rho
Wenny Rahayu
Uyen Trang Nguyen

Hindawi Publishing Corporation
Advances in Multimedia
Volume 2015, Article ID 439020, 10 pages
http://dx.doi.org/10.1155/2015/439020

Research Article

Supporting Image Search with Tag Clouds: A Preliminary Approach

Francesco Guerra, Giovanni Simonini, and Maurizio Vincini

DIEF, University of Modena and Reggio Emilia, Via Vivarelli 10, 41125 Modena, Italy

Correspondence should be addressed to Maurizio Vincini; maurizio.vincini@unimore.it

Received 9 September 2014; Accepted 11 December 2014

Academic Editor: Seungmin Rho

Copyright © 2015 Francesco Guerra et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Algorithms and techniques for searching in collections of data address a challenging task, since they have to bridge the gap between the ways in which users express their interests, through natural language expressions or keywords, and the ways in which data is represented and indexed. When the collections of data include images, the task becomes harder, mainly for two reasons. From one side the user expresses his needs through one medium (text) and he will obtain results via another medium (some images). From the other side, it can be difficult for a user to understand the results retrieved; that is why a particular image is part of the result set. In this case, some techniques for analyzing the query results and giving to the users some insight into the content retrieved are needed. In this paper, we propose to address this problem by coupling the image result set with a tag cloud of words describing it. Some techniques for building the tag cloud are introduced and two application scenarios are discussed.

1. Introduction

The numbers around Twitter are impressive: the official statistics (https://about.twitter.com/company, August 2014) state that 500 million messages are sent per day by 271 million monthly active users. Tweets are now considered as an important medium adopted by governments and enterprises for their direct communications. Therefore, Twitter constitutes a large and authoritative information repository: to be able to gain any insight into it is of paramount importance.

In this field, we are not at step zero. Finding tweets containing related information, discovering trends, and analyzing impacts/influences of users and messages are still hot, open, and challenging research topics, although effective and efficient solutions have been developed and implemented in commercial tools. Applications, platforms, and appliances performing analytics on tweets are now commercialized and adopted in real business scenarios. These tools represent the outcomes achieved by the application of big data analysis (BDA) techniques to tweets. In this area, the academic and enterprise research communities have jointly put a large effort in the development of techniques for discovering unknown correlations and hidden patterns from huge amounts of data.

These software applications are typically oriented to the analysis of text and metadata which constitute a tweet. Nevertheless, tweets can include also images that can convey interesting information for the users too. Techniques and tools for the analysis of images associated with tweets are less advanced and some research work is still needed. If we consider, for example, three of the most used applications for searching images published in Twitter, that is, the search engine available in the official website, TwiPho (http://twipho.net/), and Topsy (http://topsy.com/), users can formulate query through a simple user interface which allows them to express their interests by means of keywords. The tools return a list of images which are related to the keyword queries according to some algorithm. Nevertheless, to understand why an image has been included in the result list for a specific query is often a mystery to the user. Let us suppose, for example, that a user is querying the Twitter interface looking for images about Modena and expecting as a result photos about this Italian city. It is not easy for a user to understand why some of the top images retrieved and shown in Figure 1 are connected to the Modena city. We can justify the presence of vinegar bottles and Ferrari cars in the results since Modena is the city where they are produced, but

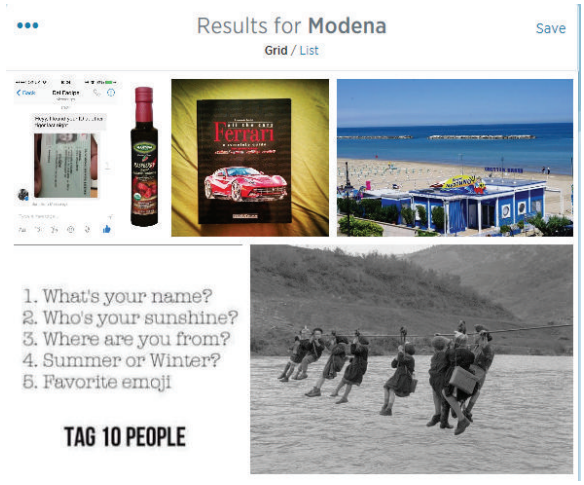


Figure 1: The top images resulting by the query "Modena" in Twitter.

the connection with Modena and the beach (last image in the first row) is hard to justify, since Modena is not close to the sea. The absence of effective techniques for analyzing the images in Twitter constitutes a tremendous gap since it has been estimated that around 36% tweets include images.

Therefore, we think that providing users with some techniques for analyzing the images retrieved by a user query is needed. Informal user studies at Yahoo!, as reported in [1], indicate that augmenting related suggestions with concrete explanations would significantly increase the relevance of the suggestions and increase user engagement. According to these studies, we claim that users would have a great benefit if they are able to couple the image result set with some justification concerning its relevance to the user query. In this paper, we discuss the abstract problem of generating tag clouds describing result sets and we propose techniques for generating tag clouds of words summarizing and explaining the images retrieved by a query. A tag cloud is a visual representation of text data associated with the images where the importance of each tag is shown with font size or color. The use of tag clouds for summarizing the results of a user query has been studied in the literature even if not frequently adopted in the image search, where we devise a two-step process for (1) tokenizing—the goal of this step is to associate images with some representative words—and (2) tag cloud generation—this step provides an effective tag cloud by using the words identified by the first step.

In some cases, the first step can be trivial: the words associated with the images are manually provided by the users publishing the image. This is the case of Flickr, one of the most used websites for hosting and sharing images and videos, which allows users to include several tags for each shared image and provides a system for searching images related to some specific user-provided tag. When you perform this kind of search in Flickr (https://www.flickr.com/photos/tags), the images returned to the users are shown along with some other tags which represent elements "related" to the tags searched. Even if a tag cloud is shown, this kind of information does not provide any insight into the images included in the result set. Also Twitter allows users to tag messages and these words (or, in case of their absence, some representative words in the message can be extracted by means of some NLP technique) can be used as input for a tag cloud generator system.

The second step needs to address two main issues: the development of techniques for the selection of which words to visualize in the tag cloud (typically a tag cloud is composed of around 40 words and the union of the tags associated with the images belonging to a result set can have a higher cardinality) and the definition of the shape (e.g., size, font, and color) to assign to each word. We claim that the process for generating tag clouds is the result of the application of three fundamental operations: (a) the selection; that is, we need functions that can reduce the total number of tags which are associated with a result set; (b) the ranking; that is, we need techniques able to order tags with respect to some metrics; and (c) the partition, that is, techniques for grouping tags. We conceive these operations as "abstract procedures": obviously there are several possible implementations for each operation, each one addressing a specific goal. For example, ranking can take into account the publication time or the frequency of a tag for ordering.

In this paper, we introduce a novel tag-based system supporting the search of images published with some textual information. Two particular use cases where the system has been implemented will be shown: MediaPresenter, a system for the creation of multimedia presentations, and an image search engine for Twitter. Our goal is to provide a tool for analyzing an image result set: for this reason our proposal can be conceived as an add-on to be coupled with the image search engine. For the sake of simplicity, we consider only images having some descriptive hashtag in the tweet. This will be used by our system to generate the tag cloud. Nevertheless, NLP techniques for extracting the most representative words of a tweet can be used for this purpose. Our idea, which extends our previous proposal [2], is to model hashtags as a network, where two tags are linked if they are associated with the same image, and to provide users with specific implementations of the fundamental operations. Our system will allow users to select and combine these operations and their specific implementations to generate a tag cloud (or a set of tag clouds) representing the images of interests. With reference to the previous example, the user can apply a partition function to the hashtags associated with the images of Modena and discover that images are related to 3 main topics: cars, vinegar, and monuments. Moreover, he can apply a ranking function and creating a tag cloud where the elements are ordered on the basis of their frequency.

The rest of the paper is structured as follows. The next section introduces some related work. Section 3 describes the model underlying the proposal and Section 4 introduces the functional architecture of the system and two use cases where the application has been implemented. Finally, Section 5 introduces some conclusions and future work.

2. Related Work

The problem of selecting a limited number of tags representing a result set has been studied in the literature and in [3]

a model and some metrics for generating tag clouds from a set of labels have been proposed. Tag clouds generated according to the proposed techniques were implemented as part of CourseRank [4]: a social tool to access official university information and statistics.

Other interesting approaches include PubCloud [5], a project that uses tag clouds for summarizing query result of PubMed biomedical literature database. The tag clouds are generated from words extracted from the paper abstracts of the query results. The font size of the words in the cloud is calculated just using terms frequency, and the set of visualized tags are obtained by using the tags having frequency higher than 10% of the best frequency: both the score and the visualized set computation are very simple with respect to other approaches, such as our technique. In [6] three different approaches to determine word cloud generation from web search results are used: full-text, query biased, and anchor text based clouds. They define a specific model to score the terms and a greedy algorithm to select best tags: preliminary results are obtained by using 2009 TREC Web Track as documents set evaluation. Moreover, the Rex system [1] is somewhat related to the motivation of our research. In the paper the need of providing explanation for keyword queries result is highlighted. We think that tag cloud can provide this information. Finally, concerning keyword search over tags, the proposed technique takes some inspiration from our previous work on keyword search over relational databases where two prototypes have been proposed [7, 8].

3. The Model

In this section we describe the data representation model enabling the generation of tag clouds through the primitive operations. We consider a set of images C and the set of tags T associated with it. In our model, tags associated with images are represented as a graph, where the nodes are the tags and an edge exists in tags cooccurring in the same image. Inspired by [3], we propose and model some measures to be applied to our graph model for the generation of effective tag clouds. Our goal is to provide a technique, based on the selection, ranking, and partitioning operations, to generate and evaluate tag clouds that summarize the results retrieved by the image search engine. We are not interested in how these results are generated or ranked by the search application: our work is independent of the way the result set is computed. In this way our proposal is applicable to any system for image search. Moreover, in this section we intend to describe a general model and the operations that can be performed exploiting it. The actual implementation of the system is based on this model and it employs only a subset of the proposed measures.

Let us assume that a query q is a subset of T: this is a reasonable assumption since, typically, from a query q, an image search engine returns a collection of images $C_q \subseteq C$ and the set of tags T_q associated with at least one image $c \in C_q$. We denote by $A(t)$ the association set of the images that are tagged with a tag t and belong to C.

Definition 1 (association set of t under q). One defines the association set $A_q(t)$ of a query q as $A_q(t) = A(t) \bigcap C_q$.

In order to provide a flexible model to generate tag clouds, we consider the general definition of a scoring function:

$$s: C_q \longrightarrow [0, 1]. \tag{1}$$

A straightforward scoring function is the frequency of an image in $c \in C_q$. Employing it, all images have the same score equal to $1/|C_q|$, where $|C_q|$ is the cardinality of C_q. We call this function frequency function $f(\cdot)$. Other scoring functions can be exploited in order to give more importance to some images rather than others, for instance, assigning a higher score on the basis of the timestamp of the image: the more a photo is recent the more it is relevant, while older photos could also be not considered under a certain threshold. Other scoring functions can be taken into account: spatial proximity (with respect to the user's position) and the "social level" of the results (measured, e.g., by the number of retweets in Twitter).

Given a scoring function $s(\cdot)$, we want the space of tags T_q as a graph of tags $G_q(V, E, \Pi, \Gamma)|_s$ where V represents the vertices and each vertex is a tag $t_i \in T_q$; E is an edge between two tags $t_i, t_j \in T_q$ with $i \neq j$ that cooccurs in an image $c \in C_q$; Π and Γ are, respectively, the set of weights of the vertices and the set of weights of the edges. The weight of a node is defined as follows:

$$w_{t_i} = \sum_{c_i \in A_q(t)} s(c_i). \tag{2}$$

Intuitively, if $s(\cdot) = f(\cdot)$, the weight of a node t_i represents the fraction of images that belong to C_q and are tagged with t_i. Then, we define the weight w' of a pair of tags and use it to define afterwards the weighs of the edges:

$$w'_{t_i,t_j} = \sum_{c_k \in A_q(t_i) \bigcap A_q(t_j)} s(c_k). \tag{3}$$

Once again, if $s(\cdot) = f(\cdot)$, then w'_{t_i,t_j} represents the cooccurrence of the two tags t_i and t_j, normalised for the total number of images $|C_q|$. The w'_{t_i,t_j} can be directly used as weight w_{t_i,t_j} of the edge between two tags in G_q; alternatively, it allows computing other measures to be exploited as weights of edges in G_q. In fact, the computation of Dice, Jaccard, and Cosine coefficients becomes straightforward:

$$\begin{aligned} \text{Dice}_{t_i,t_j} &= 2 * \frac{w'_{t_i,t_j}}{w_{t_i} + w_{t_j}} \\ \text{Jaccard}_{t_i,t_j} &= \frac{w'_{t_i,t_j}}{w_{t_i} + w_{t_j} - w'_{t_i,t_j}} \\ \text{Cosine}_{t_i,t_j} &= \frac{w'_{t_i,t_j}}{\sqrt{w_{t_i} * w_{t_j}}}. \end{aligned} \tag{4}$$

Formally, a tag cloud S is a subset of T_q, represented in our model as a subgraph G_S of the graph G_q of tags under a query

q that summarizes the query results and aims to help the users in the navigation of them. In order to quantitatively evaluate the goodness of a tag cloud we define below two measures: the coverage and the overlap of S.

3.1. Evaluation. The coverage $\mathrm{cov}(S)$ of a tag cloud S is a measure of the fraction of images belonging to C_q that are associated with tags of S:

$$\mathrm{cov}(S) = \frac{W_S - I_S}{W_{C_q} - I_{C_q}}, \tag{5}$$

where I_P and W_P are, respectively, the weight of the inner edges and the weight of the inner nodes of a set of vertices P:

$$I_P = \sum_{\substack{t_i,t_j \in P \\ t_i \neq t_j}} w_{t_i,t_j}, \qquad W_P = \sum_{t_i \in P} w_{t_i}. \tag{6}$$

The coverage of a tag cloud S depends on the number of images $c_i \in C_q$ that are associated with tags belonging to S and their score $s(c_i)$. If $s(\cdot) = f(\cdot)$ and $w = w'$, then the coverage of S represents the exact fraction of images of C_q associated with at least one tag of S.

Another measure we take into account evaluating a tag cloud is the overlap $\mathrm{overlap}(S)$ of S that can be seen as a measure of redundancy, that is, how many images associated with a tag $t_i \in S$ are associated also with another tag $t_j \in S$:

$$\mathrm{overlap}(S) = \frac{I_S}{W_S}. \tag{7}$$

Generally, a desirable tag cloud should have a low overlap and a high coverage. Below we define and discuss about some metrics useful to perform the selection and ranking of T_q in order to build S.

3.2. Ranking and Selection. To perform the ranking and the selection of nodes belonging to the graph of tags $G_q(V, E, \Pi, \Gamma)|_s$, we need to determine the importance of a node within the network. If the importance can be measured, both selection and ranking of nodes can be performed basing on it.

We can consider nodes with a high number of connections (also considering the weight of those connections) to be important. A measure that captures this idea is the centrality degree $D_c(t_i) = \sum_{t_j \in T_q} w_{t_i,t_j}$ that can be normalised by the maximum degree d_j in the network, or by the degree sum I_c.

Another possible approach is to compute the PageRank of the nodes in the graph, relying on the idea that if an important node is connected to another node, the latter should be important too.

All these measures lack one aspect: they tend to consider all nodes belonging to a unique cluster that have to be summarized. This is a quite contrived assumption that rarely fits for real cases. In fact, generally the results can be classified in different clusters due to the intrinsic ambiguity of the tags. Hence, besides allowing a partitioning and a ranking task, we need a further step: the partitioning.

3.3. Partitioning. Many algorithms can be employed to partition a graph [9]. The goal of this task is to minimise the overlap among different clusters and at the same time maximise the strength of the association of the members inside a cluster. To give a quantitative measure, according to the previous notation, we define the group clustering coefficient as

$$\mathrm{cluster}(S) = \frac{I_S - \beta B_S}{W_S}, \tag{8}$$

where $B_S = I_C - I_S$ is the sum of the weights of the edges that link a node inside to one outside the cluster.

Similarly, our model allows to exploit community detection algorithms, in particular [10] that proposes a technique to identify automatically the optimal number of communities, as well generating hierarchical or overlapping ones.

4. The System

Our application is conceived as two separate components that work coupled: a search engine retrieving images and related tags and a cloud generator that analyzes the results provided by the first tool to generate a summarized view in the form of a tag cloud of the contents. The components are independent of each other: the generation of the tag clouds does not rely on the technique adopted for retrieving the images, but it only takes into account the images and tags retrieved and, vice versa, the image searching is not influenced by the tag cloud generation process. Moreover, working with images and related tags is not a limitation, since there are applications working in real scenarios managing and retrieving images and related words.

Figure 2 shows the functional architecture of the searcher and the tag cloud generator components. In our preliminary prototype, the searcher component actually returns images on the basis of the associated descriptions. As shown in the figure, the first operation performed by the component is the collection of images and related descriptions. The goal of this step is to generate tags which are representative of the images starting from their descriptions. The component implements a simple information retrieval technique, based in particular on vector spaces [11], for retrieving and ranking images on the basis of their descriptions with respect to user keyword queries.

The input of the second component is the result of the user keyword query computed by the searcher, with the aim of generating its representation in the form of tag cloud. The technique proposed models the result set as a graph where nodes are the tags and edges exist between tags associated with the same image. Moreover, the nodes in the graph are weighted on the basis of their frequency. Starting from this graph representation of the result a tag cloud is generated by the application of the three fundamental operations of selection (to reduce the number of tags), ranking (to discover the most important ones and to visualize them accordingly), and partition (to cluster tags which are in some way related). There are a number of possible implementations of these operations, which are based on and try to maximize different

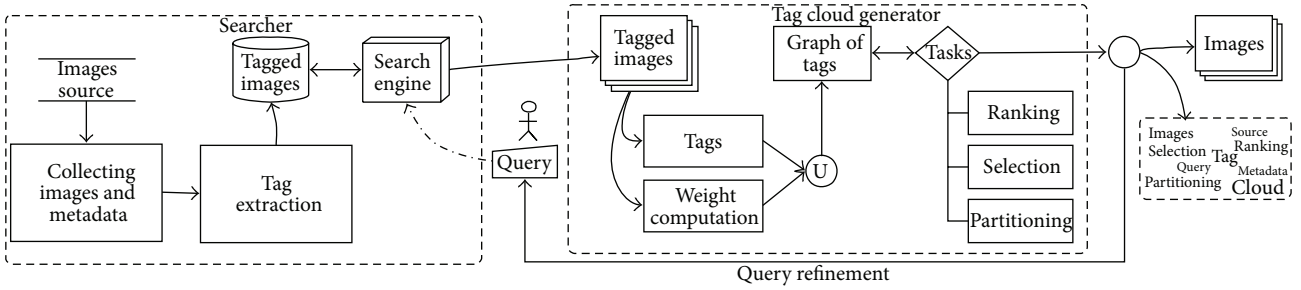


Figure 2: The functional architecture of our application.

measures. In the following, we will propose some proposals as they have been implemented in our prototypes. Moreover, we think that it is a responsibility of the user to choose which operation to apply (only one operation or a series of them), the order of their execution, and the specific implementation.

A first implementation of our idea has been proposed and tested in MediaPresenter, a tool developed through a join collaboration between the DBGroup at University of Modena and Reggio Emilia and Addiction Creation Media Lab, an Italian SME. Part of the activity has been funded by Italian Emilia Romagna region, within the LISEA laboratory (http://spring.bologna.enea.it/lisealab/). As described in Section 4.1, the tag cloud generated in this project is obtained as the result of a selection process only and by using a measure. In Section 4.2, we show our ideas implemented in MediaPresenter can be extended for dealing with the retrieval of images in Twitter.

4.1. MediaPresenter. MediaPresenter is an online cross-platform application, which offers a large number of services for sharing and managing digital archives. The main goal of MediaPresenter is to produce multimedia presentations and this could be done by combining multimedia resources available in a repository called MediaBank. We experimented our ideas for supporting image search with tag cloud in MediaPresenter by implementing a service supporting users in retrieving interesting contents from the MediaBank repository. Other services are offered by MediaPresenter and they include the concurrent access to data by multiple users with different roles, the possibility of importing multiple types of digital resources (3D representations, videos, images, etc.) and exporting them in various formats (swf, pptx, png, and pdf), and a keyword-based search engine for retrieving digital contents from MediaBank. The process for generating presentations consists of four steps, namely, selection, assembling, transformation, and presentation.

The Selection Step. In this step, the multimedia resources contained in the MediaBank are retrieved using a information retrieval technique based on vector space. Each multimedia resource in the repository is identified by a unique code (typically the name of the file) and has associated a series of metadata which specify contents and the properties that characterize such element. The metadata constitute the search space where the IR technique looks for the keywords provided by the user as an input.

The Assembling Step. In this step, the user assembles the final presentation starting from the single resources retrieved in the previous step. Users can also assemble different types of elements depending on their role. For instance, one user can be a slide-maker and therefore he can assemble just slides; meanwhile a presentation-maker can assemble only complete presentations.

The Transformation Step. Once the user has repeated iteratively the previous steps and the complete presentation has been created, the transformation step allows him to save the final product in different formats according to the user needs.

The Presentation Step. MediaPresenter client has been developed as a Flex application running inside a browser; hence a presentation can be potentially shown on whatever device having a browser and an Internet connection. Nevertheless, a presentation can be published in different formats, and consequently it can be shown through other applications.

4.1.1. The MediaPresenter Tag Cloud. The main goal of MediaPresenter is to support users in publishing multimedia presentations. To reach this goal, the system provides the user with all the available information about the topic which can be briefly summarized in presentations, unpacked slides, or series of slides and digital resources already used in the past or available as digital content of the enterprise. During the creation process, the typical action performed by users is searching resources stored into the MediaBank using name, dimension, type, and date of creation as search criteria. The results from these searches are often unsatisfactory, mainly due to the lack of database structure knowledge and experience of the user. Furthermore, database search results are often considered as database tuples, whereas nontechnical people think in terms of entities, not tuples. To overcome this issue, we devised a particular search method which allows users to perform a keyword search over the MediaBank database using terms that can be found in different fields (name, title, description, etc.) and in multiple relations, hiding the data structure to the user. In order to make this approach even more effective, the system enables users to

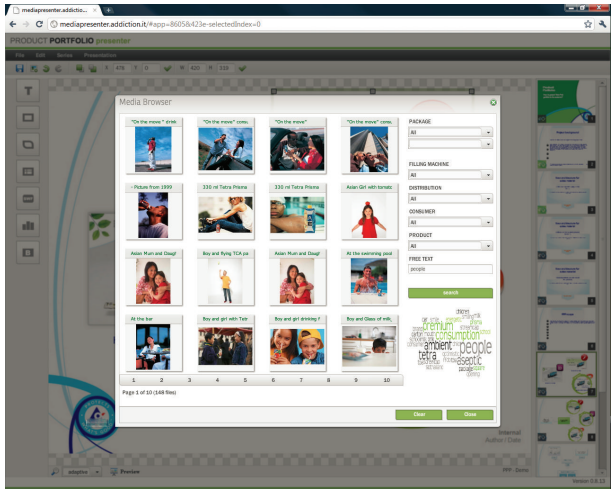


Figure 3: The MediaPresenter GUI.

associate words to each digital resource: these tags that can be manually specified by the users choosing the correct ones among a predefined set of proposals or creating new tags ex novo at run-time. The action of organizing resources by adding metadata is called "tagging" and it is gaining popularity on the web in these years [12]. Using tags to annotate resources allows the system not only to specify the keyword search over the stored assets, but also to create tag clouds and to consider each term in the cloud as a hyperlink that can be used to refine the search results, dynamically guiding users in the hidden relationship among contents and eventually leading to serendipitous discoveries of interesting results.

Figure 3 shows the MediaPresenter interface used for keyword searching supported by tag clouds. In this case the user was looking for all the multimedia resources containing the term "people." The user can select the preferred resource on the left, and the tag cloud at the bottom right of the image supports the user in browsing all the related resources.

4.1.2. Keyword Search over the MediaBank and Tag Cloud Generation. In this section, the process adopted in MediaPresenter for keyword search and tag cloud generation is introduced. Let us denote by D the MediaBank database part where the search process is applied and by R_i the ith relation stored in D. Each relation contains a set C of columns. We consider $R_i \cdot C_j$ as the jth column of the ith relation. By t we denote a generic tuple in D. Given R_i and R_j and a primary-foreign key relationship between R_i and R_j, we consider TD as the tuple graph of the database D, where for nodes we consider each tuple in D and given two tuples $t_i \in R_i$ and $t_j \in R_j$, an edge exists among them if $(t_i \bowtie t_j) \in (R_i \bowtie R_j)$. D can be modeled as a collection V of search entities. In our case V corresponds to the set of digital assets that can be returned by the search method, providing, thus, a sort of unit of representation for returned entities. For each entity $v \in V$ we consider C_i as the ith attribute describing the entity. C_i can be seen both as a one-to-one mapping to a particular column in the database

Table 1: The MediaBank fragment containing data searchable by the users.

(a) `DAM_object`

Asset_ID	Asset_name	Folder_name	Asset_file_name
DA001	asset_001	Products	box_front.jpg
DA639	opening_3	Packages	B03240.jpg
DA640	opening_4	Packages	ustraws.jpg

(b) `tag`

Tag_ID	Term
T45	Yellow
T10	Box machine
T55	Products
T2	Umbrella
T19	Aseptic
T31	Juice
T50	Square
T87	Operator

(c) `serie_slide`

Slide_ID	Title	Source
S33	Overview	<mx:Application> ...
S101	Special box	<mx:Application> ...
S6	Conclusions	<mx:Application> ...
S869	Updates	<mx:Application> ...

(d) `presentation_serie_template`

Object_ID	Name	Description
P50	The new box machine	In this presentation...
P13	About MediaPresenter	MediaPresenter is a...

(e.g., the resource name) and also as a many-to-one mapping, therefore grouping several information in one search entity attribute (e.g., the set of tags specified for a digital asset can be thought as an attribute of the asset entity). In particular, we consider C_0 as the identifier of each specific search entity. An entity ID, hence, is a mapping to the primary key of the relation R_0, where R_0 is called primary entity relation. In our context, we recognize as primary entity relation the table `DAM_object`, which provides all the digital resource IDs. On the other hand, we call all the other relations that join directly or indirectly with R_0 and provide additional information to v secondary entity relation. We identify tag, `presentation_serie_template`, and `serie_slide` tables as secondary entity relations. Table 1 depicts the database relations we took into account for the keyword search.

Summarizing, the keyword search engine we developed returns digital resources identified by the ID stored in the `DAM_object` primary relation. Each resource contains attributes directly related to the primary relation (name, file name, folder name) but also attributes grouping information belonging to secondary relations. Each entity gets information about the slide(s) it belongs to, thanks to the join with the `serie_slide` relation. In addition, information

about the presentation (series, template) is added joining the relation `serie_slide` with `presentation_serie_template`. At the end the relation tag provides information about the set of assets tags as well as information about the set of tags related to the presentation (series, template) containing the asset entity.

The input of our search function is a query q, and we assume that q is composed of a certain number of keyword terms. We assume that given a keyword term k and a search entity v identified by the ID stored in the tuple t of the primary relation R_0 and v contains k if one of the following statements holds: (a) one of the attributes values of t contains k; (b) TD contains a tuple t_i stored in the relation R_i that contains an attribute value equal to k, and a path in the tuple graph connecting the tuple t_i to t exists. Given a query q, the set of resulting entities is denoted by $V_q \subseteq V$, and it contains the set of search entities related at least to a keyword term k contained in q.

In this application, we proposed the selection operation for generating the cloud from the tags associated with the multimedia resources. For this purpose, let us consider the set L of all tags. These tags are textual labels (words) assigned to a resource; thus each resource $v \in V$ is associated with a set of tags, denoted by L_v. We denote by L_q the set of tags related to the entities contained in V_q; similarly we consider $V_q(l) \subseteq V_q$ as the set of objects associated with the tag $l \in L_q$. Following the coverage measure introduced in [3] we implemented a tag selection algorithm to maximize the number of entities in V_q that are covered by the set of tags $S \subseteq L_q$ resulting as output. In addition, since the user creates tags in a context of a group and each group has a label identifying its generic topic, we can consider that given a certain search result, the sum of all the groups' labels is itself a tag cloud summarizing all the topics of the results. In order to sum up the tag clouds resulting from the tags and the one resulting from the group labels, we use colors to identify for each tag the group it belongs to and an index showing all the groups related to the search. In this way the user is able to perform a refinement over the results using two different levels of granularity: by generic topic, selecting the group of interest on the index, and one more detailed using the tags from the cloud.

4.2. Searching for Images in Twitter. Twitter offers a second use case of where to apply our ideas for supporting search for images by means of tag clouds. Our work in this scenario is still preliminary: for the moment we have developed a software prototype and we are now evaluating the user experience in using our techniques.

Twitter already provides a search engine; nevertheless, as observed in the introduction, in some cases it is not clear in which way images are related to the user keyword queries. We claim that a tag cloud can support the user in this process, by providing some insight into the contents of the image result sets. This knowledge can furthermore be exploited for refining the keyword queries, by adding terms better reflecting the intended meaning of the user and improving the quality of the results. Our idea is to implement our technique as an add-ons application that analyzes the result obtained by the Twitter search engine. With reference to the functional architecture in Figure 2, the first component is already implemented by Twitter and we have focused our effort on the second component. There are two main issues that have been addressed for the development of the system: (1) the definition of the "candidate tags" for a tweet and (2) the development of a GUI for managing the user interaction and some implementation of the three fundamental operations to be used in this context.

Concerning the first point, the issue is to define which tags are associated with an image. Twitter allows users to define specific tags, called "hashtags"; nevertheless in our experience the use of only this metadata is limiting since it is not adopted by users. In our testing dataset (obtained by a random selection by real posts published on Twitter), only 23% of tweets with an associated image have also some hashtags. For this reason, our choice was to consider as tags all the words part of the tweet, after the removal of stop words and a stemming process. In this way, the number of tags associated with each image increased. If needed (this was not the case for our experiment), to reduce the noise generated by irrelevant words, it is possible to reduce the number of tags by considering, in the graph generations, only terms that appear as more than a specified threshold.

Figure 4 shows the GUI supporting users in the tag cloud generation. The interface is divided into two parts. In the main part the images retrieved by the Twitter search engine, as an answer to the user keyword query formulated through the input text box at the top, are shown along with their tag cloud. A simple dashboard allows users to select which operations, which implementation of them, and in which order they are to be executed for the generation of the cloud. In the right part of the GUI, the system shows what happens, in terms of images retrieved and tag cloud, with a number of automatic computed refinements of the user query. The suggestion of new possible keywords directly derives the process for generating tag clouds, where the best results (according to the metrics selected by the user) can be added to the original ones. In this case the application shows three refinements, but the number can be specified by the user. In this way, we devise an iterative process, where the user can manually refine his queries or be supported by the application in finding what he is looking for.

There are some possible metrics that can be used for the implementations of the selection, ranking, and partition operations. Table 2 shows some metrics that we have exploited to develop techniques dealing with Twitter images. In particular, techniques based on the analysis of space and time proximity can be exploited for implementing versions of all the operations. By using techniques based on these measures we can select, rank, and group tags on the basis of their spatial/temporal proximity. According to these measures, for example, we can assign high priority to the most recent tags. Techniques based on frequency can be used for selecting and ranking tags. For example, we can exploit the coverage degree (i.e., the amount of images which are associated with a subset of the tags [3]) and the overlap degree (see Section 3) for selecting the tags which better summarize the images to be inserted in the tag cloud. Since tags are

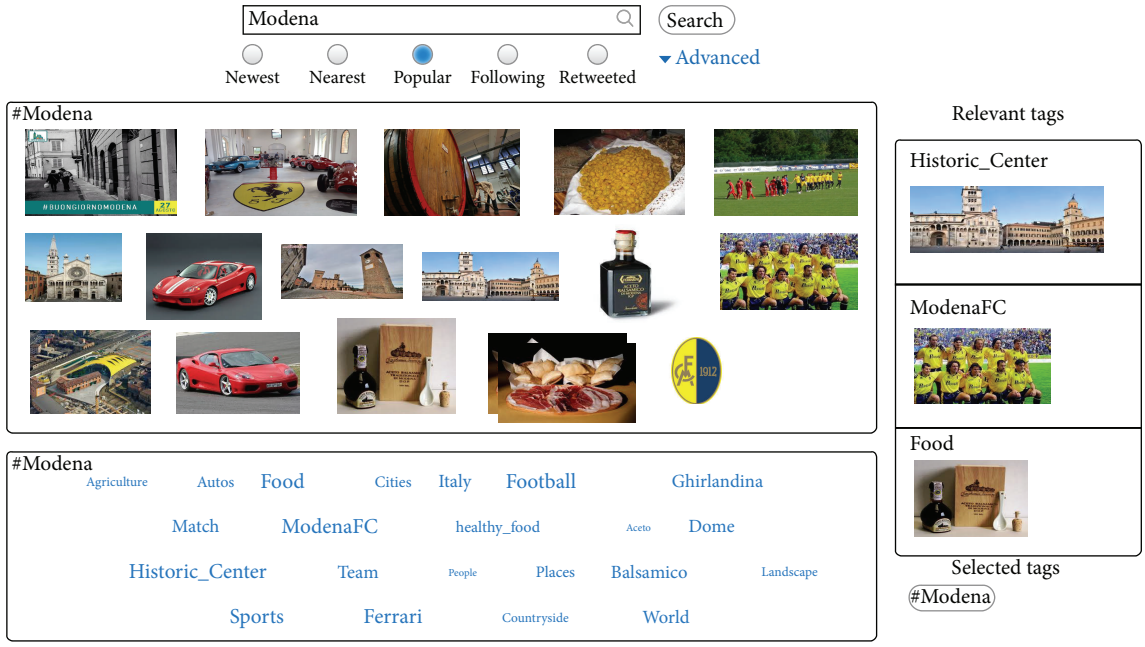


Figure 4: The GUI of the tag cloud generator adapted for Twitter.

Table 2: Some possible implementation of the fundamental operations.

Metrics	Selection	Ranking	Partition
Space/time proximity	X	X	X
Frequency	X	X	
Link analysis	X	X	X
Semantic analysis	X		X

Table 3: Selected tags associated with the query "Modena."

Selected tags
Agriculture, vehicles, autos, race, food, Italian, cities, Italy, football, match, ModenaFC, healthy_food, aceto, dome, Historic_Center, Maranello, team, grapes, people, university, places, Balsamico, sports, Sassuolo, pasta, restaurants, winery, wine, Ferrari, Ghirlandina, square, ham, stadium, landscape, Enzo_Ferrari, museum, countryside, world

modeled as a graph, we can exploit metrics which have been developed in the field of link analysis for all the operations. In Section 3, the centrality degree and PageRank have been proposed for analyzing the graph representation. Techniques based on these values can be exploited for the selection, ranking, and partitioning of the tags. Finally, semantics-based technique can be used for identifying tags which are similar, or representing more/less generic concepts than other ones.

4.2.1. Motivating Example. As a motivating example, we address the keyword query "Modena" to our system, and we show how the tag cloud associated with the results can be generated exploiting the proposed operations of selection, ranking, and partitioning. First of all the system retrieves all the images that are associated with the tag "Modena" and collects all the tags associated with them.

Starting from the list of tags, the system computes the cooccurrence and similarity metrics and builds the graph of tags. Finally, a selection operation is performed trying to minimize the overlap of the tags while selecting those with higher degree centrality. Table 3 shows the selected tags. All these tags are then ranked, on the basis of their importance, measured with the PageRank. Visually the notion of importance is expressed by means of the font size of tags shown to the user. To better summarize the content of the tag cloud, the set of tags are partitioned exploiting a community detection algorithm. This allows the tool to manage the intrinsic ambiguity of a query, since the retrieved images are about different topics. In our example, the community detection algorithm identifies four main topics: the food, the Modena football team, the Ferrari cars, and the city of Modena and its historical center (see Table 4).

The analysis of the search task highlighted by this motivating example shows that the combination of selection, ranking, and partitioning procedures provided by our proposal can really support users in effective and efficient keyword search in Twitter images.

To the best of our knowledge, the procedures provided by our approach and the support that it can provide in the search process are not available in any other tool. A qualitative comparison of our proposal with some of the available commercial keyword search systems for images is shown in Table 5. In particular, we formulated the same keyword query

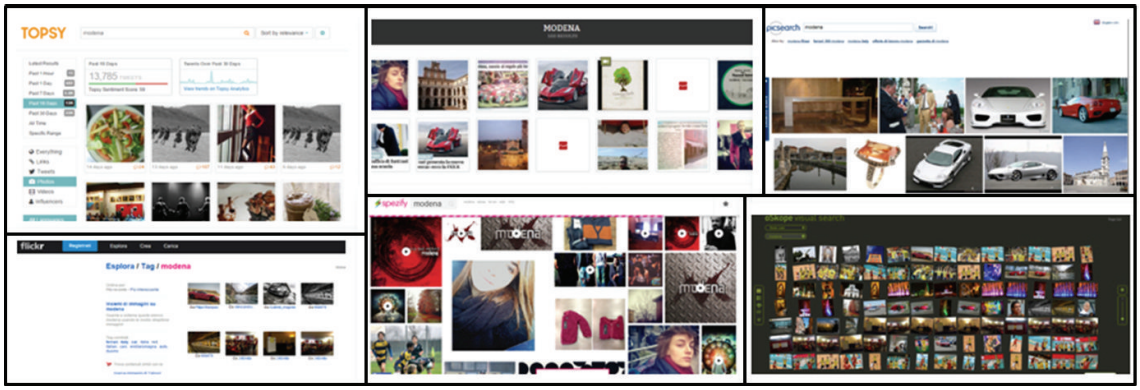


Figure 5: The six tools under evaluation.

Table 4: Partitions of the tag cloud.

Partitions	Tags
City	Italian, cities, Italy, dome, Historic_Center, people, university, Sassuolo, Ghirlandina, square, landscape, countryside, world places
Car	Vehicles, autos, race, Maranello, Ferrari, museum, Enzo_Ferrari
Football	Football, match, ModenaFC, team, stadium, sports
Food	Agriculture, healthy_food, aceto, grapes, Balsamico, pasta, restaurants, winery, wine, ham, food

Table 5: Qualitative comparison of well known tools.

Website	Images	Tags	Tags—images	Tag expl.
Topsy	2	n.a.	n.a.	n.a.
TwiPho	1	n.a.	n.a.	n.a.
Picsearch	2	1	2	2
Flickr	2	1	1	3
Spezify	3	2	2	n.a.
oSkope	1	n.a.	n.a.	n.a.
Our proposal	2	1	1	1

("Modena") to the tools: Topsy (http://topsy.com/), TwiPho (http://twipho.net/), Spezify (http://www.spezify.com/), Picsearch (http://www.picsearch.co.uk/), Flickr (https://www.flickr.com/photos/tags), and oSkope (http://www.oskope.com/). The results provided by the tools and shown in Figure 5 have been analyzed and compared with the ones obtained by our proposal according to four perspectives: quality of the images retrieved (i.e., we evaluated if the images provided as a result can be easily associated in some way with the subject of the query), quality of the tags retrieved (i.e., we evaluated if some tags are provided as a result and if they can be easily associated in some way with the images and the subject of the query), relationships between tags and images (i.e., we evaluated if images and tags retrieved are in some way related), tag explorations (i.e., we evaluated if and in which way the system supports search for related tags). For each perspective and each system, a rating (1—strongest, 3—weakest) is provided if the feature is implemented.

Topsy, oSkope and TwiPho are tools oriented only to image retrieval: they do not provide any tag or justification for the answers returned to the user. The evaluation reported in Table 5 represents the accuracy obtained by analyzing the relevance of the images in the result set. In our experiments, TwiPho and oSkope performed better than Topsy. Picsearch, Flickr, and Spezify associate tags with the images. In our experiments, Spezify was not able to retrieve accurate results both in terms of images and in terms of tags. Moreover, the tags proposed are lowly related to the query (i.e., the system generated the tags "Modena," "stamp," "Ferrari," "stati," and "1852." Among these tags, only Modena and Ferrari are related to the query). Flickr and Picsearch are the tools which performed better in our experiments; nevertheless, in both the tools, searching for tags produces new queries which are only poorly related to the initial user's request.

5. Conclusion and Future Work

In this paper, we have presented our approach for coupling result sets with tag clouds. We think that the knowledge conveyed by the tag cloud can be extremely useful to provide to the user a better insight into the relevance of the result set. This knowledge is really helpful when users are looking for images, where typically there is a mismatch between the way the users formulate queries (by text) and the results obtained (images). In this scenario, finding a connection between query and answer can be hard. We have introduced our preliminary ideas and we have shown how these ideas have been implemented in two systems. The next steps of our research are mainly two: (1) to develop new techniques for implementing the selection, ranking, and partition operations for the tag cloud generation and (2) to evaluate the user experience in using our approach, with particular reference to the Twitter scenario.

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

References

[1] L. Fang, A. D. Sarma, C. Yu, and P. Bohannon, "Rex: explaining relationships between entity pairs," *Proceedings of the VLDB Endowment*, vol. 5, no. 3, pp. 241–252, 2011.

[2] S. Bergamaschi, F. Ferrari, M. Interlandi, and M. Vincini, "Mediapresenter, a web platform for multimedia content management," in *Sistemi Evoluti per Basi di Dati—SEBD 2011, Proceedings of the Nineteenth Italian Symposium on Advanced Database Systems, Maratea, Italy, June 26-29, 2011*, G. Mecca and S. Greco, Eds., p. 437, 2011.

[3] P. Venetis, G. Koutrika, and H. Garcia-Molina, "On the selection of tags for tag clouds," in *Proceedings of the 4th ACM International Conference on Web Search and Data Mining (WSDM '11)*, pp. 835–844, February 2011.

[4] B. Bercovitz, F. Kaliszan, G. Koutrika et al., "Social sites research through courserank," *SIGMOD Record*, vol. 38, no. 4, pp. 29–34, 2009.

[5] B. Y.-L. Kuo, T. Hentrich, B. M. Good, and M. D. Wilkinson, "Tag clouds for summarizing web search results," in *Proceedings of the World Wide Web Conference (WWW '07)*, pp. 1203–1204, 2007.

[6] R. Kaptein and J. Kamps, "Word clouds of multiple search results," in *Multidisciplinary Information Retrieval*, vol. 6653 of *Lecture Notes in Computer Science*, pp. 78–93, Springer, Berlin, Germany, 2011.

[7] S. Bergamaschi, E. Domnori, F. Guerra, M. Orsini, R. T. Lado, and Y. Velegrakis, "Keymantic: semantic keyword-based searching in data integration systems," *Proceedings of the VLDB Endowment*, vol. 3, no. 2, pp. 1637–1640, 2010, http://www.comp.nus.edu.sg/~vldb2010/proceedings/files/papers/D31.pdf.

[8] S. Bergamaschi, F. Guerra, M. Interlandi, R. T. Lado, and Y. Velegrakis, "QUEST: a keyword search system for re lational data based on semantic and machine learning techniques," *Proceedings of the VLDB*, vol. 6, no. 12, pp. 1222–1225, 2013.

[9] S. Fortunato, "Community detection in graphs," *Physics Reports*, vol. 486, no. 3–5, pp. 75–174, 2010.

[10] Y.-y. Ahn, J. P. Bagrow, and S. Lehmann, "Link communities reveal multiscale complexity in networks," *Nature*, vol. 466, no. 7307, pp. 761–764, 2010.

[11] W. B. Croft, D. Metzler, and T. Strohman, *Search Engines—Information Retrieval in Practice*, Pearson Education, 2009.

[12] S. A. Golder and B. A. Huberman, "The structure of collaborative tagging systems," http://arxiv.org/abs/cs/0508082.

Hindawi Publishing Corporation
Advances in Multimedia
Volume 2015, Article ID 498408, 8 pages
http://dx.doi.org/10.1155/2015/498408

Research Article

An Empirical Analysis of Technology Transfer of National R&D Projects in South Korea

Mi-Sun Kim,[1] Dong-Ho Shin,[1] Jae-Soo Kim,[2] and Byeong-Hee Lee[2]

[1]*Korea University of Science and Technology (UST), 217 Gajeong-ro, Yuseong-gu, Daejeon 305-350, Republic of Korea*
[2]*Korea Institute of Science and Technology Information (KISTI), 245 Daehak-ro, Yuseong-gu, Daejeon 305-806, Republic of Korea*

Correspondence should be addressed to Byeong-Hee Lee; bhlee@kisti.re.kr

Received 28 August 2014; Accepted 27 October 2014

Academic Editor: Seungmin Rho

Copyright © 2015 Mi-Sun Kim et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

This study is aimed at seeking policy implications for the policy makers of South Korean government and finding a direction to support R&D institutions in performing R&D activities more efficiently, by analyzing the factors influencing technology transfer of the national R&D projects. The data retrieved from NTIS (National Science & Technology Information Service) was used in analyzing the results of 575 projects with 1,903 cases of technology transfer, performed by the Ministry of Science, ICT and Future Planning, between 2002 and 2012. We found that there were significant differences between the government funded institutions and the universities and between basic R&D and applied ones. We also discovered that the government funded institutions did not necessarily take a better position than the universities in terms of the quantity of technology transfer. Lastly, the applied R&D of the universities was very vulnerable in terms of technology transfer.

1. Introduction

The interest in the technology transfer has increased, as the R&D scopes have been wider and the territories among the industries have been loosened. Technology transfer is defined as the flow of the technology from an entity to another one [1, 2], and it is also defined as the transfer of the physical assets, know-how, and the technical knowledge [3]. Other definitions look at technology transfer as a proactive process, in which the obtained knowledge, experiences, or the outcomes are diffused into the society [4]. In addition, Mittelman and Pasha [5] explained the technology transfer as the flow from the creation of knowledge, skills, organizations, values, or capital to their stabilized applications through its introduction. To facilitate the flow of technology, several countries set up a legal framework. With regards to technology transfer related laws, Stevenson-Wydler's Technology Innovation Act in 1980 and Federal Technology Transfer Act in 1986, in America, set up the framework to connect the producers of the knowledge and its users. The regulations allowed setting CUFT, The Center for the Utilization of Federal Technology, inside NTIS (National Technical Information Service) to facilitate efficient technology transfer and have enforced that at least more than 0.5% of the R&D budget has to be spent on technology transfer. They set technology transfer as one of the important government duties and have strived to facilitate it by reflecting it in the evaluation of the government [6]. In the case of Korea, a movement to increase efforts in facilitating the technology transfer was initiated in 2000, along with the technology transfer promotion act. Many studies were conducted to encourage technology transfer: however, the most of these studies have only focused on the system and were not able to boost technology transfer, although the related infrastructures were built up, thanks to them [7]. In order to resolve this problem, in 2014, Korean government announced to invest approximately 9 hundred billion KRW (approx. 900 million USD) to provide support for technology transfer by 2017, which meant increasing up to 4.0% of the total R&D investment amount [8]. The purposes of this budget increase are to facilitate the circulation of research outcomes and to strengthen the relationship between research and its applications. The values of the R&D projects depend on creating and utilizing R&D outcomes, through which national R&D projects aimed to aid the national development [9]. Although science and technology is often not able to produce outcomes quickly, the failure in R&D should be

accepted as necessary, and there would be various ways to utilize the results. However, the final goal of R&D should be to make a contribution to national development through creating and utilizing the fruits of the successful R&D.

In 2014, we should now contemplate on the utilization of the technologies, as Korea has heavily invested on science and technology, which almost has the highest investment rate on R&D against GDP [10], and has been able to achieve high growth rate in a short period, thanks to science and technology. Therefore, this study was aimed at empirically analyzing the results of the technology transfer of national R&D projects in Korea. We believe that the outcomes of this study would be useful in drawing attention to policy implications for the policies to efficiently support and manage the creation and utilization of the R&D outcomes. We will review the technology transfer of national R&D projects, supported by Korean government, by the types of R&D organizations, and by the types of R&D. Then, we will propose the policy implications in which the national R&D supporting policies are efficiently applied, respectively, by the types of R&D organizations and by the types of R&D. We will also review how the lead-time from the completion of R&D to the technology transfer affects the royalties, the benefits of the technology. Lastly, we propose the direction of the policies for the technology transfer by tracing the results of national R&D projects with the same purpose to diffuse R&D outcomes.

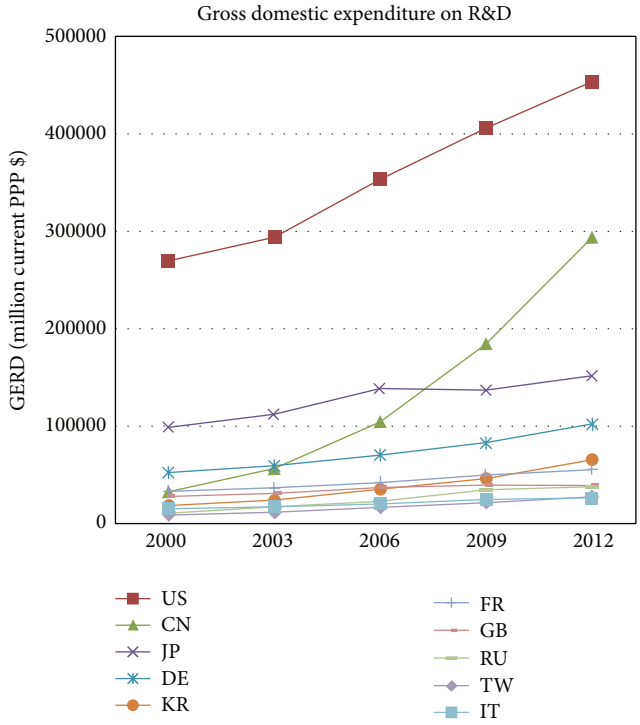


Figure 1: Gross domestic expenditure on the R&Ds (reedition of OECD's data in 2014).

2. Concepts and Global Trends

There is a growing trend in the investment amounts in R&D all over the world. The investment in R&D is increasing not only in industrial sector but also in national R&D projects. Figure 1 shows the gross domestic expenditure on R&D (GERD) of several major countries in the world. Approximately 41% of the total GERD in OECD countries was spent by America, and main 7 countries, that is, America, Japan, Germany, Korea, France, UK, and Italy, invested about 80% of the GERD of the total 34 OECD countries, in R&D. Among non-OECD countries, China, Russia, and Taiwan were also shown to heavily invest in R&D, almost at a comparable level with that in the above 7 countries.

Figure 2 shows GERD against the economic scales of each country. It presents the R&D investment amount against GDP, based on the data given by OECD in July 2014. When the average of OECD was taken as "1," Korea invested 1.8 times more than the average of OECD and comparatively small countries, such as Israel, Finland, Sweden, and Korea, showed high percentages of R&D investment against their GDPs.

Then, do they make enough direct gains from the technologies or indirect ones by creating, such as a new technology market by utilizing them, as they heavily invested on R&D? According to the report of the Korean Ministry of Commerce, Industry and Energy, Korea has only a half of the technology transfer, compared to the main technologically advanced countries, America or European ones [7]. It could be explained by closed culture of Korea in which people do not take advantage of existent technologies for their research. Also we suspect the lack of efficient tracking system on national R&D projects and excessive administrative work that may lead to weak outcomes and become a hindrance for efficient research. There are several reasons why technology transfer is difficult to achieve; these include the following: (1) there are differences between the universities and the industries in R&D methods and (2) there are again discrepancies between them in terms of the R&D goals or objectives [11]. In addition, national R&D projects in Korea have continuously increased in number and in size, except for the types of supporting organizations. They increased from 108 in 1998 to 408 in 2012, and the related budget also rose sharply from 1,942,500,000,000 won (billion and 950 million USD) in 1998 to 10,744,500,000,000 won (10 billion and 750 million USD) in 2012 [12]. We need to pay attention to the efficiency of the investments and the structure of the projects, as the scales of the national R&D projects are bigger. With regards to the above mentioned trend, Kwon et al. [13] analyzed the factors influencing the 21th century frontier R&D project, one of the national R&D projects. Whether the types of the R&D organizations, the types of R&D, the lead-time of R&D, or the field of the R&D projects showed the differences in the outcomes was analyzed and it was found that the universities had the high research paper outcomes, the industries had the high rate of patent applications and registrations, and the long-term researches with 6 years and more had the high rate of patent applications. However, Kwon et al. [13] had a limitation in that it counted only the technology transfer related contracts, which failed to consider the qualitative outcomes of the technology transfers. So far, the studies on the project unit have been frequently conducted. However, this study will review the relation between the types of

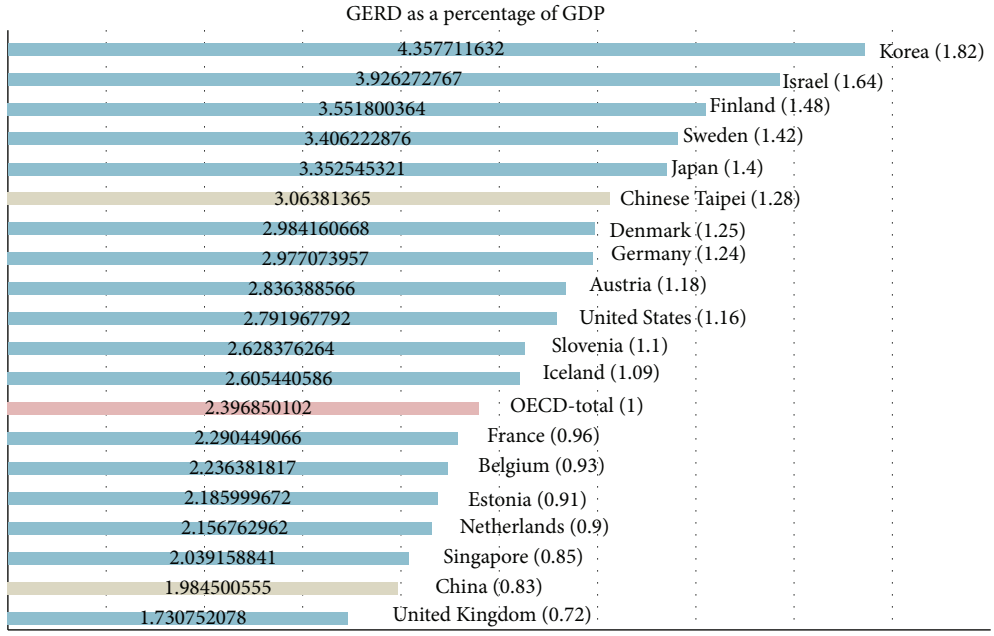


Figure 2: The proportion of GERD against GDP.

the R&D organizations, the types of R&D and the lead-time from the completion of R&D to technology transfer, and the transfer, with the overall outcomes of the national R&D projects by the Ministry of Science and Technology in Korea [14].

3. Hypotheses

The study sets up hypotheses as shown below to analyze the factors influencing the technology transfer of the national R&D projects in Korea.

Hypothesis (1): There Is a Significant Difference in Technology Transfer by the Types of the R&D Organizations. Depending on who conducts R&D, that is, the universities, the government-funded research institutes, or the industries, the purposes of the activities and the characteristics of the participants are different. When applying the same criteria to the all R&D organizations, having different R&D directions and purposes, it is equivalent to a molding with an already fixed frame regardless of differences. In the study by Cohen et al., he emphasized on the fact that there was a clear difference between the universities' innovation and that of the industries [15–18]. In this regard, Rosenberg and Nelson [11] addressed that the difficulty in bringing the R&D outcomes to the market was the difference in R&D between universities and industries, and the transfer of the outcomes between them was difficult to achieve, as their R&D activities had different focuses and goals. In addition, when [13] analyzed the outcomes of the 21th century frontier R&D project, one of the national R&D projects, he addressed that the universities had the high research paper outcomes and the industries had the high rate of patent applications and registrations and interpreted the analysis results were due to the fact that the universities and the industries had the different viewpoints from each other in their R&D activities.

Table 1: The R&D development stages.

R&D development stage	Criteria
Basic R&D	Originally conducted, a theoretical or experimental R&D to obtain a new knowledge on the observable objects or the natural phenomena, without any purpose of a special application or industrialization
Applied R&D	An R&D initiative to obtain new scientific knowledge mainly with a practical purpose or goal, utilizing the knowledge given by basic R&D
Development R&D	A systematic research to substantially improve the products, which are already produced or set, or to produce a new product or equipment by utilizing the knowledge obtained from basic, applied R&D or actual experience
Others	Other R&D activities, which do not belong to any of the above categories

Hypothesis (2): According to the Types of R&D, There is a Significant Difference in the Outcomes of Technology Transfer. OECD divides R&D types into the basic, the applied, and the development types [19]. NTIS in Korea also collects the related basic, applied, development, and other research data, in accordance with the criteria of OECD, shown in Table 1.

Grimaldi and von Tunzelmann [20] proved that the applied R&D had clear success factors, compared to the basic R&D, by analyzing LINK program, which was a big scaled

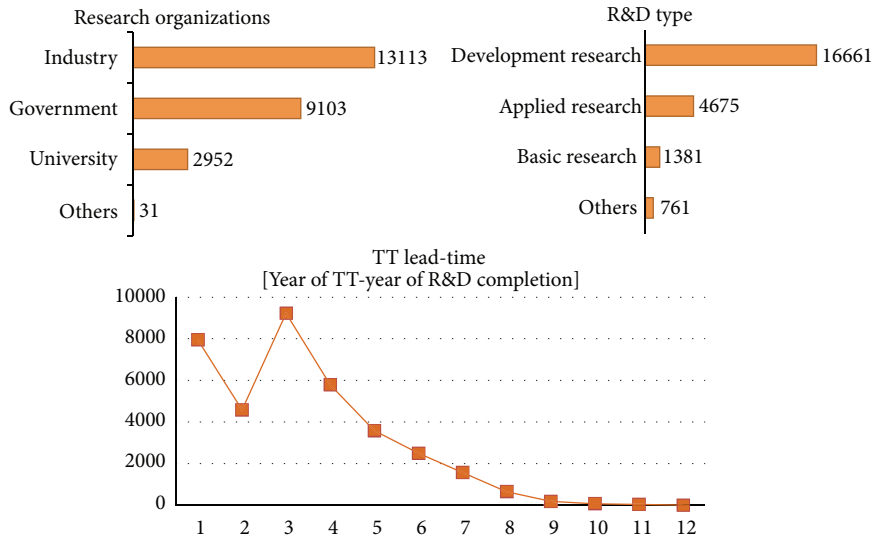


Figure 3: The outcomes of the technology transfer (TT) of the overall national R&D projects.

R&D project in UK. Although the study was only limited to the big scaled R&D project, we believe that it will be applicable in the overall technologies, and according to the characteristics of the each R&D type, the outcomes of R&D may be different. Therefore, it is applicable in analyzing the differences in the technology transfer by the types of R&D.

Hypothesis (3): According to the Lead-Time from the Completion of R&D to Technology Transfer, There is a Significant Difference in the Outcomes of the Transfer. From the study result that the long-term R&D had more domestic patent applications than the short-term R&D [12], the above hypothesis is set up to analyze the influence of the lead-time from the completion of R&D to the technology transfer. Also this hypothesis aimed to look at data pattern related to the time elapsed between the research and the utilization of the technology. The lead-time is defined from the starting year of the research to the year of the transferred technology. Consequently this study could give stakeholders a basis for a suitable policy to evaluate the project period and the expected outcomes.

4. Research Methodology and Data

4.1. Basic Statistics Data. This study utilized the data of NTIS (National Science & Technology Information Service), which collected the information and data, including the goals, the participants, the facilities, and the outcomes, of the national R&D projects run by 17 ministries and administration (16 representative specialists) of South Korea, and data analysis was performed with R package. The data was collected from 2002 as the starting year of the projects and from 2006 as transferred year, on the basis of 23,478 cases opened to the public by 2012. From the analysis of the data, we found that small or medium sized businesses which is industry in Figure 3 dominated in the technology transfer covering about 51% of the total transfer and the development research transfer covered 71% of the total transfer, as shown in Figure 3, TT refer to technology transfer. We decided to only focus on the technology transfer done by the Ministry of Technology, ICT and Future Planning, the technology related government organization, to avoid the study biasing towards the outcomes produced by the small or medium sized businesses.

Figure 4 shows the technology transfer done by the Ministry of Technology, ICT and Future Planning, on the basis of analyzing 575 projects with 1,903 cases of technology transfer from 2002 to 2012. The transfer by the ministry through their projects was 56.38% to the universities, 40.25% to the government-funded research institutes, and 2.9% to the industries and mainly concentrated on applied R&D. In cases of the industries, mostly the transfer was done from the projects by small and medium business administration to small or medium sized businesses, and it was unique that the transfer was approximately 73% in the same years of the projects.

4.2. Variables and the Summary of the Statistics. In analyzing the outcomes of the technology transfer of the national R&D projects, this study sets the number of the transfer and the royalties with the transfer as the dependent variables of R&D outcomes and sets the types of R&D organizations, the R&D types, and the lead-time of the technology transfer as the independent variables. The details of the variables in this study are shown in Table 2.

In Table 2, the lead-time from the completion of R&D to the technology transfer was calculated by deducing from the year of the technology transfer to the completion year of R&D. The summary statistics on each variant is shown in Table 3; in the types of R&D organizations, G refers to the government, I to the industries, and U to the universities; in the R&D types, B refers to basic R&D, A to applied R&D, and D to development R&D, and Time means the lead-time from the completion year of R&D to the year of technology transfer. The coefficient variables (CV) show that

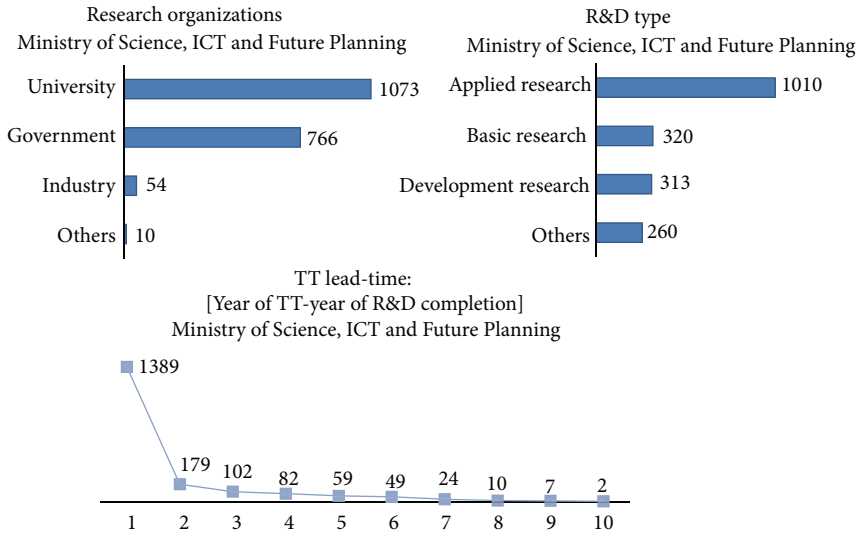


Figure 4: The outcomes of the technology transfer by the science and technology related ministry of the national R&D projects.

Table 2: The categories of the variables and the details.

Independent variable	Type of research organization (a)	Government-funded research institutes (1), industry (2), and universities (3)
	R&D type (b)	Basic research (1), applied research (2), and development research (3)
	Lead-time from the completion of R&D to technology transfer (c)	0 years to 8 years
Dependent variable	Number of technology transfer cases (A)	The contracts for the technology transfers during the above mentioned period
	Royalties (B)	The technology transfer related royalties, set with sections

the variation of each independent variable is getting bigger with the number of the transfer than with the royalties.

4.3. The Analysis Methodology. This study was aimed at finding a direction to improve the policies related technology transfer and facilitating efficient R&D activities and transfer, by analyzing the outcomes of the transfer of the national R&D projects, by the types of R&D organizations, by the R&D types, and by the lead-time of the technology transfer. The normality should be verified to analyze the influences of the types of the R&D organizations, that is, the government-funded research institutes, the industries, and the universities on the number of the technology transfer (TT) and the royalties. As the normality was not valid, Kruskal-Wallis test, as nonparametric one, was applied for the further analysis. It was the same for the analysis of the R&D types. If a significant difference was found through Kruskal-Wallis test, the data was analyzed with Kruskalmc to find which independent variable particularly influenced the specific dependent ones [21]. The lead-time from the completion of R&D and to the technology transfer was analyzed with regression analysis, as the lead-time was continuous.

5. The Analysis Results

The study results validated the above addressed 3 hypotheses. In Section 5.1, the 1st hypothesis, which was about the case if the types of the R&D organizations brought a significant difference in the outcomes of technology transfer, and the 2nd hypothesis, which was about the case if the types of R&D caused a significant difference in the outcomes of the transfer, were tested with 5% significance level. In Section 5.2, the 3rd hypothesis, which was about the case if the lead-time of the technology transfer had a significant difference, was reviewed.

5.1. The Analysis of the Outcomes by the Types of R&D Organizations and the Types of R&D. The results of the normality test with 5% significance level are shown in Table 4. Table 5 shows Kruskal-Wallis test results and the test was applied, as there was no normality in all conditions, that is, between A-a, A-b, B-a, and B-b.

As shown in Table 5, the number of the technology transfer (TT) (A) shows a significant difference with the types of the organizations (a) and the types of R&D (b) in Kruskal-Wallis test. However, royalties (B) does not show a

Table 3: The summary of basic statistics.

(a)

Dependent variable	Type of organization	N	Mean	S.D.	CV
Number of TT (A)	G(a1)	301	1.3986	1.324	0.9467
	I(a2)	37	1.2162	0.479	0.3938
	U(a3)	237	2.194	2.932	1.3364

(b)

Dependent variable	Type of organization	N	Mean	S.D.	CV
Royalties (B)	G(a1)	301	7.847	5.844	0.7447
	I(a2)	37	10.000	6.868	0.6868
	U(a3)	237	8.068	6.028	0.7471

(c)

Dependent variable	R&D type	N	Mean	S.D.	CV
Number of TT (A)	B(b1)	159	2.235	2.954	1.3217
	A(b2)	264	1.189	0.597	0.5021
	D(b3)	152	1.362	1.064	0.7812

(d)

Dependent variable	R&D type	N	Mean	S.D.	CV
Royalties (B)	B(b1)	159	8.458	5.941	0.7024
	A(b2)	264	7.057	5.842	0.8278
	D(b3)	152	8.480	6.165	0.7270

(e)

Dependent variable	Taken time	N	Mean	S.D.	CV
Royalty (B)	Time (c)	575	1.318	1.864	1.4143

Table 4: Normality test.

Dependent variable	Independent variable	Result
Number of TT (A)	Organization (a)	P value $< 2.2e-16$
	R&D type (b)	P value $< 2.2e-16$
Royalties (B)	Organization (a)	P value $= 5.041e-16$
	R&D type (b)	P value $= 1.669e-15$

significant difference with 5% significance level with the types of the organizations (a), and types of R&D (b) is close to the significant level $\alpha = 0.05$, which means that it is just statistically significant.

The results of postmortem analysis of Kruskalmc, to compare which type of the organizations shows the difference with the technology transfer, are shown in Table 6. The table also shows the multiple analysis results on the relation between the 3 different types of the organizations and the technology transfer and the royalties. First, the 1st hypothesis, which was about the case if the types of the R&D organizations, that is, the government-funded research institutes, the industries, and the universities, brought a significant difference in the outcomes of the technology transfer, was partially proved. The reason why it was only partially proved is that the significant difference was only shown with the number of the transfer but not with the royalties. Particularly, the number of the transfer clearly shows the significant outcomes between the universities and the government-funded research institutes, while it does not show any significant outcomes between the government-funded research institutes and the industries or the universities and the industries. The industries belong to the 2 results without statistical significances; it can be interpreted as they conduct the related R&D activities from the initial stages, according to their own purposes, and therefore, they have very strong purposes to utilize the technologies by themselves rather than transfer, which is obviously different from the universities and the government-funded research institutes. Second, the 2nd hypothesis, where the types of R&D, that is, the basic, the applied, and the development R&D, brought a significant difference in the outcomes of the transfer, was proved. Particularly, the observed values between the basic R&D and the applied R&D and the number of the technology transfer and the royalties were greater than the verification threshold, which were all statistically significant. However, the development research group was not significantly different from the basic research group and the applied research one.

Through the above analysis, this study found that there were significant differences between the number of the technology transfer and the universities and the government-funded research institutes and between the number of the transfer and the basic R&D and the applied R&D. Therefore, 4 groups, that is, the government-funded basic R&D, the government-funded applied R&D, the universities with the basic R&D, and the universities with the applied R&D, were compared through multiple comparison analysis and the following are the results. The results of analysis are shown in Table 7.

If the types of R&D were additionally considered with the types of the R&D organizations, (1) government-funded basic R&D had the higher numbers of the transfer than the universities with the applied R&D. However, the result could not be considered significant when it was compared with that of the universities regarding basic R&D. (2) Government-funded applied R&D showed the higher numbers in the transfer than the one of the universities with the applied R&D. However, again it could not be considered as significant when it was compared with the one of the universities with the basic R&D.

5.2. The Analysis of the Outcomes by the Lead-Time of the Technology Transfer and the Types of R&D. The results of the analysis on the lead-time of the technical transfer applied regression analysis are shown in Table 8. The 3rd hypothesis is accepted as royalties according to the fact that the lead-time was statistically significant. However, the persuasiveness was very weak with 1%, as it was difficult to generalize

Table 5: Kruskal-Wallis test.

Dependent variable	Independent variable	Result	
Number of TT (A)	Organization (a)	$X^2 = 19.3439$, df = 2	P value = $6.303e-05^{***}$
	R&D type (b)	$X^2 = 25.885$, df = 2	P value = $2.394e-06^{***}$
Royalties (B)	Organization (a)	$X^2 = 3.4139$, df = 2	P value = 0.1814
	R&D type (b)	$X^2 = 6.9971$, df = 2	P value = 0.03024^{*}

Signif. codes: $^{***}P < 0.001$, $^{**}P < 0.01$, and $^{*}P < 0.05$.

Table 6: Multiple comparison.

Dependent variable	Independent variable			Obs. dif.	Critical dif.	Difference
Number of TT (A)	Organization (a)	G	I	0.97543	69.28660	False
		G	U	46.01721	34.53892	**True**
		I	U	45.04138	70.30323	False
	R&D type (b)	B	A	60.56925	39.92498	**True**
		B	D	21.71808	45.11644	False
		A	D	38.85118	40.49468	False
Royalties (B)	R&D type (b)	B	A	41.63243	39.92498	**True**
		B	D	39.42918	45.11644	False
		A	D	2.20325	40.49468	False

Table 7: Multiple comparisons considering the types of R&D.

Dependent variable	Independent variable		Obs. dif.	Critical dif.	Difference
Number of TT (A)	GB	UA	103.35820	78.13171	**True**
	GB	UB	7.91700	85.77833	False
	GA	UB	20.39063	75.24104	False
	GA	UA	75.05057	66.39168	**True**

Table 8: Simple linear regression test.

Dependent variable	Independent variable	y-Intercept	Gradient	R^2	Ra^2	F(df)	P value
Royalties (B)	Lead-time (c)	7.6086	0.3549	0.01217	0.01045	7.061	0.0081^{**}

Signif. codes: $^{***}P < 0.001$, $^{**}P < 0.01$, and $^{*}P < 0.05$.

it with the weak persuasiveness. The results signified that responding to the flow of the markets and the technologies with flexibility, rather than forecasting the lead-time of the technology transfer in advance before starting R&D, would increase the efficiency of the transfer in both quantity and quality. However, it will be worth comparing it with the results with the bigger parameter. The study significantly showed that long-term projects brought positive economical results rather than an adventure in the end. At the same time, the study showed that too much speculated technologies and R&D periods would not be necessarily positive in generating revenue.

6. Conclusion

The study reviewed the outcomes of national R&D projects by the types of R&D organizations and by the types of R&D and analyzed the factors influencing the outcomes. The purpose of the study was to propose the direction of the policies for the technology transfer by tracing the results of the national R&D projects with the same purpose. Therefore, this study analyzed how the outcomes of the technology transfer influenced the number of the transfer and the royalties, by the types of R&D organizations and by the types of R&D, and what the relation between the lead-time from the completion of R&D to the technology transfer and the royalties was. As the analysis result, we found there were significant differences between the government-funded R&D institutions and the universities and the basic R&D and the applied R&D. The 4 groups, that is, the government-funded basic R&D, the government-funded applied R&D, the universities with the basic R&D, and the universities with the applied R&D, were compared through multiple comparison analysis. The results of the analysis showed that the government-funded basic R&D had the higher numbers of the transfer than the universities with the applied R&D. However, the result could not be considered significant, when it was compared with the one of the universities with the basic R&D. The government-funded applied R&D showed the higher numbers in the transfer than the one of the universities with the applied R&D. However, again it could not be considered significant when it was compared with the one of the universities with the basic

R&D. It signified that the government-funded institutions and the universities had the open possibility of the technology transfer as they had relatively the character of public interest or influence. They showed statistically significant difference in royalties. However, the persuasiveness was very weak which implied that they considered the technology transfer as the public assets rather than their own economic benefits. On the other hand, it was interpreted as their R&D purposes were about the technology transfer itself, rather than generating the economic values through the transfer. The analysis result of the types of R&D organizations with the consideration of the types of R&D showed that the government-funded R&D institutions may not always have a better position over the universities in terms of quantity of the technology transfer and also demonstrated that the universities with the applied R&D projects were very weak in terms of technology transfer. Further study is required to check a trigger to facilitate the technology transfer by the universities with the applied R&D and also validate the qualitative relation with R&D budget. With regard to the qualitative relation, Ok and Kim [22] analyzed that R&D budgets clearly influenced the number of the technology transfer, the royalties, and the number of the new technologies, and the individual R&D capacity (the number of the SCI articles per head) was also statistically significant in raising the efficiency of the transfer of the universities. Although the study was about the outcomes of the universities, it would be also very interesting if it is compared with the economic values with input and output on the national R&D projects.

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

Acknowledgments

This research was supported by the Sharing and Diffusion of National R&D Outcome funded by the Korea Institute of Science and Technology Information.

References

[1] W. E. Souder, A. S. Nashar, and V. Padmanabhan, "A guide to the best technology-transfer practices," *The Journal of Technology Transfer*, vol. 15, no. 1-2, pp. 5–16, 1990.

[2] K. Ramanathan, "The polytrophic components of manufacturing technology," *Technological Forecasting and Social Change*, vol. 46, no. 3, pp. 221–258, 1994.

[3] B. Bozeman, "Technology transfer and public policy: a review of research and theory," *Research Policy*, vol. 29, no. 4-5, pp. 627–655, 2000.

[4] A. P. Hameri, "Technology transfer between basic research and industry," *Technovation*, vol. 16, pp. 51–57, 1996.

[5] J. H. Mittelman and M. K. Pasha, *Out from Underdevelopment Revisited: Changing Global Structures and the Remaking of the Third World*, St. Martins Press, New York, NY, USA, 1997.

[6] R. C. Dorf and K. K. F. Worthington, "Models for commercialization of technology from universities and research laboratories," *The Journal of Technology Transfer*, vol. 12, no. 1, pp. 1–8, 1987.

[7] C. Y. Lim and Y. J. Lee, *An Analysis for Success Factor of Technology Transfer: From GRI's Perspectives*, STEPI, 2007.

[8] The Ministry of Science, ICT, and Future Planning of Republic of Korea, "The technical commercialization promotion planning for R&D result diffusion," 2014.

[9] D. B. Chung and D. D. Jung, "The effects of performance management & application capabilities and activities on technology transfer from Public Research Institutes in Korea," *Journal of Technology Innovation*, vol. 21, pp. 199–223, 2013.

[10] OECD, July 2014, http://www.oecd.org/statistics/.

[11] N. Rosenberg and R. R. Nelson, "American universities and technical advance in industry," *Research Policy*, vol. 23, no. 3, pp. 323–348, 1994.

[12] Y. S. Ko, "The analysis of the process of the structural change in national R&D projects," The Survey Report, KISTEP, 2014.

[13] J. C. Kwon, J. B. Moon, Y. J. Yoo, and C. G. Lee, "Achievement characteristic analysis for large scale government R&D projects focusing on 21st century frontier R&D program," *Journal of Korea Technology Innovation Society*, vol. 15, pp. 185–202, 2012.

[14] M. S. Kim, D. H. Shin, J. S. Kim, and B. H. Lee, "Performance analysis on technology transfer in national R&D project," in *Proceedings of the International Conference of on Convergence Content (ICCC '14)*, vol. 12, pp. 5–6, June 2014.

[15] W. M. Cohen, A. Goto, A. Nagata, R. R. Nelson, and J. P. Walsh, "R&D spillovers, patents and the incentives to innovate in Japan and the United States," *Research Policy*, vol. 31, no. 8-9, pp. 1349–1367, 2002.

[16] R. C. Levin, A. K. Klevorick, R. R. Nelson, and S. G. Winter, "Appropriating the returns from industrial research and development," *Brookings Papers on Economic Activity*, vol. 1987, pp. 783–831, 1987.

[17] E. Mansfield, "Academic research and industrial innovation," *Research Policy*, vol. 20, no. 1, pp. 1–12, 1991.

[18] D. C. Mowery and B. N. Sampat, "The Bayh-Dole Act of 1980 and university-industry technology transfer," *Journal of Technology Transfer*, vol. 30, no. 1-2, pp. 115–127, 2004.

[19] OECD, "Frascati Manual," 2002.

[20] R. Grimaldi and N. von Tunzelmann, "Sectoral determinants of performance in collaborative R&D projects," *International Journal of Technology Management*, vol. 25, no. 8, pp. 766–778, 2003.

[21] S. Siegel and N. J. Castellan, *Nonparametric Statistics for the Behavioral Sciences*, McGraw-Hill, 1988.

[22] J. Y. Ok and B. K. Kim, "Measuring the performance of technology transfer activities of the public research institutes in Korea," *Journal of Technology Innovation*, vol. 17, pp. 131–158, 2009.

Hindawi Publishing Corporation
Advances in Multimedia
Volume 2015, Article ID 420848, 4 pages
http://dx.doi.org/10.1155/2015/420848

Research Article

Development of Ontology and 3D Software for the Diseases of Spine

Seungbock Lee,[1] Sangho Lee,[1] Dongmin Seo,[1] Kwan-Hee Yoo,[2] and Sukil Kim[3]

[1]*Software Research Center, Korea Institute of Science and Technology Information, Daejeon 305-806, Republic of Korea*
[2]*Department of Digital Information Convergence, Chungbuk National University of Korea, Cheongju 361-763, Republic of Korea*
[3]*College of Medicine, The Catholic University of Korea, Seoul 137-701, Republic of Korea*

Correspondence should be addressed to Sukil Kim; sikimmd@gmail.com

Received 28 August 2014; Accepted 18 November 2014

Academic Editor: Seungmin Rho

Copyright © 2015 Seungbock Lee et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

KISTI is carrying out an e-Spine project for spinal diseases to prepare for the aged society, so-called NAP. The purpose of the study is to build a spine ontology that represents the anatomical structure and disease information which is compatible with simulation model of KISTI. The final use of the ontology includes diagnosis of diseases and setting treatment directions by the clinicians. The ontology was represented using 3D software. Twenty diseases were selected to be represented after discussions with a spine specialist. Several ontology studies were reviewed, reference books were selected for each disease and were organized in MS Excel. All the contents were then reviewed by the specialists. Altova SemanticWorks and Protégé were used to code spine ontology with OWL Full model. Links to the images from KISTI and sample images of diseases were included in the ontology. The OWL ontology was also reviewed by the specialists again with Protégé. We represented unidirectional ontology from anatomical structure to disease, images, and treatment. The ontology was human understandable. It would be useful for the education of medical students or residents studying diseases of spine. But in order for the computer to understand the ontology, a new model with OWL DL or Lite is needed.

1. Introduction

KISTI (Korean Institute of Science and Technology Information) has been studying a National Agenda Project (NAP) for developing elderly human body model for treatment and rehabilitation of age-related spinal disorders. The purpose of the study is to build a virtual human spine as a simulation model through mathematical modeling to use in virtual experiment instead of real human spine. Accurate diagnosis and treatment of spinal diseases were expected from the project. We tried to develop the spinal ontology which contains information on spine and the related diseases for the success of the main project.

Ontology is systemized process accomplished by using computers for building a model which present the recognizable concepts and the relations between them [1]. Neches et al. (1991) defined ontology as "basic terms and relations comprising the vocabulary of a topic area as well as the rules for combining terms and relations to define extensions to the vocabulary" [2] and Gruber (1993) defined it as "an explicit specification of a conceptualization" [3].

This study focused on developing spinal ontology with frequently occurring spinal diseases in Koreans. It contains anatomy of spine, method of treatment, cause, and classification information related with spine. Further, the spinal ontology can be linked to the simulation model for education of medical students and for the physicians and biomedical engineers by offering the necessary information in their fields.

2. Method

The authors are composed of a wide range of professional researchers, medical informatics, computer professionals, and clinical experts such as nurses, a neurosurgeon, and 2 imaging specialists. The research was conducted in 5 phases (Figure 1): (1) review related to existing ontology for the construction of the model, (2) selecting the spine related diseases and the subject of the research at the same time,

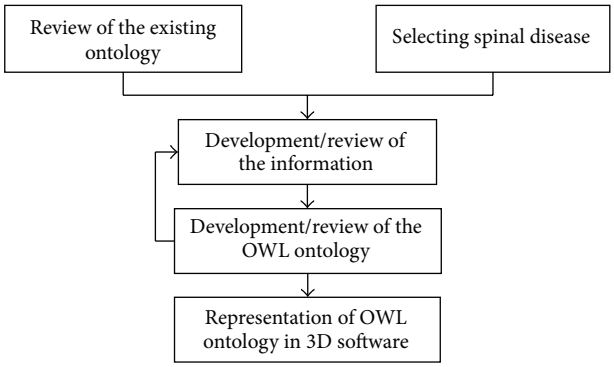


Figure 1: Process of building spine ontology.

(3) developing/reviewing spinal ontology, (4) creating OWL ontology in accordance with the clinician's feedback, and (5) Reviewing the OWL ontology by the specialists. In addition, the ontology was represented by 3D image software for the easy understanding.

2.1. Review of the Existing Ontology. We reviewed results of ontology project using Protégé which were led in 1987 as a public project at Stanford University [4]. Among their results, we gathered information that is necessary for spine ontology after analyzing the ontology of rat anatomy and classification of diseases.

2.2. Selecting Spinal Diseases. The spinal diseases were selected based on the following three criteria. First, the disease has to be one of the highly occurring spinal diseases among Koreans. Second, the disease must occur in a specific area of the spine rather than throughout the whole spine. This makes it possible for the ontology to provide information that is suitable to the characteristics of the diseases among Koreans. Also, it is much easier to link with the simulation model of KISTI which is made according to Korean human being. Last, the OWL ontology of the disease should be able to be expressed on the computer so that it can be used in clinics or medical schools for education.

2.3. Development/Review of the Information. The developed ontology was organized according to the diseases with Microsoft Excel. The anatomic definitions that consist of ontology were referenced from a medical dictionary [5] and the disease related information was extracted from publications recommended by clinicians [6]. We classified anatomical information into two categories; anatomical location and anatomic properties were represented in OWL ontology (Table 1).

Disease related information was classified into five categories as shown in Table 2; anatomical location, property of the disease, symptom/sign, method of treatment, and image were represented in OWL ontology.

The spinal ontology was reviewed by a neurosurgeon and two imaging specialists. Sample images of diseases, CT or M.R.I, were collected during the study period in Seoul St. Mary's Hospital and linked to the diseases in the ontology.

Table 1: Anatomical information represented in the ontology.

Entry	Ontology	OWL expression
Location	Anatomical location	spine: isPartOf
Properties	Part name	rdfs: label
	Anatomical classification	rdfs: subClassOf
	Standard code for the structure	spine: KOSTOM
	Definition and description of the structure	spine: definition spine: description

2.4. Development/Review of the OWL Ontology. Spinal OWL ontology was built based on OWL Full model which is a standard ontology language developed by W3C (World Wide Web Consortium). Both Altova Semantic Works and Protégé were used to build and review the OWL ontology.

In the process of OWL representation, we tried to determine the level of expression in classes (resource object) or individuals (literal object). For example, if the disease related information is "herniated nucleus pulposus", ⟨herniated nucleus pulposus⟩ is identified as superclass and ⟨cervical intervertebral disc herniation⟩, ⟨lumbar intervertebral disc herniation⟩, and ⟨thoracic intervertebral disc herniation⟩ which are classified under herniated nucleus pulposus are identified as subclass according to their location. Each class contains additional information related to their occurring region.

2.5. Representation of OWL Ontology in 3D Software. The contents of OWL ontology on spine were represented by using 3D image S/W. The software has three modules: 3D rendering module, OWL query module, and the module for showing disease information that comes from the ontology. The users may select a part of spine image of question. Then a list of the diseases from the OWL spine ontology file will appear through OWL query operation. When a disease among the list is selected, the query module searches the disease related information such as causes, symptoms, diagnoses, treatment, complication, and image of the disease.

3. Result

3.1. Selected Spinal Diseases. The list of 20 selected diseases is presented in Table 3. If scientific papers were referred in addition to text book, they were added as references in the table.

3.2. Development of the Ontology. Figure 2 presents Protégé OWL ontology graph created from the spinal ontology of the twenty selected diseases. The anatomical class represents the entire structure that composes the spine. There are 50 classes; 1 vertebral column, 5 vertebrae, 33 vertebrae, and other 11 materials of spine. Each class has 6 properties. To

Table 2: Diseases related information represented in ontology.

Entry	Ontology	OWL expression
Location	Anatomical disease location	spine: hasSite
Disease properties	Name of disease	rdfs: label
	Classification of diseases	rdfs: subClassOf
	Apply the standard code	spine: KOSTOM
	Definition of disease	spine: definition
		spine: description
	Clinical diagnosis	spine: diagnosis
	Cause	spine: hasCause
	Concomitant diseases	spine: hasConcomitantDisease
	Complication	spine: hasComplication
Symptom/sign	Symptom	spine: hasSymptom
		spine: causeOfSymptom
	Sign	spine: hasSign
Treatment	Surgical treatment	spine: hasSurgicalTreatment
	Nonsurgical treatment	spine: hasNonSurgicalTreatment
	Conservative treatment	spine: hasTreatmentConservative
Image	Preoperative image	spine: hasImageBeforeTx
	Postoperative image	spine: hasImageAfterTx

Table 3: The twenty selected diseases.

Atlas fracture	Ossification of ligament flavum
Degenerative marrow change (Modic type change)	Osteoarthritis in facet joint (Pfirman grade) [10, 11]
Grading of lumbar disc degeneration [7]	Osteoporosis
Hangman's fracture	Osteoporotic compression fracture
HNP (herniation of nucleus pulposus) [8]	Scoliosis
Infectious spondylitis	Spinal stenosis
Kyphosis	Spondyloarthropathy
Meningocele [9]	Spondylolisthesis
Odontoid process fracture	Subaxial fracture (fractures in C3~C7) [12]
OPLL (ossification of posterior longitudinal ligament)	Thoracolumbar spine fracture

express a sentence "C1 cervical is part of cervical vertebra" in OWL Full model, we defined anatomical structures "C1" and "cervical vertebra" as a class and ⟨is a part of⟩ as a property representing a predicate. ⟨Disease⟩ was defined as a superclass and the 20 selected diseases were treated as classes. As a result, 21 classes were formed for the concept of diseases and each class has 18 properties.

More than 100 images that were collected were linked to 20 diseases, one per each. The predicates that link images to the other part of ontology include ⟨hasImageBeforeTx⟩ and ⟨hasImageAfterTx⟩.

3.3. Representation of Spine Ontology in 3D Software. The user interface is composed of three parts (Figure 3). (1) 3D rendering part: the users can rotate, move, zoom in, and zoom out the whole spine on the left upper part of the window and the detail of the selected anatomical structure in a large scale is displayed on the bottom left window with its textual relationships. (2) The list of diseases: the diseases that are related with the anatomic site on the 3D rendering part are displayed on the right upper part of the window following the ontological relationship between anatomic sites to diseases. (3) The details of the disease specific information: when a disease is selected in the upper right window, the information of the disease is listed on the bottom right window, which includes disease properties, treatments, and the related diagnostic images. If there are textual descriptions on the properties, they are also displayed on the bottom right window.

4. Conclusions

We built the ontology of spine with links to the cause, symptoms, method of treatment of highly occurring spinal disease among Koreans, and anatomical information.

The completed spinal ontology expresses anatomical connection of the parts of spine and their vertical relationships as well as information on the diseases in the spine. It is easy to understand the structure and the diseases of spine by conceptualizing the anatomical structure of spine and show them in 3D images.

This study was completed by the use of literal object of OWL Full model by expressing the contents of the main reference dictionary and publications about spine literally. But in order for the computer to interpret the ontology, a new

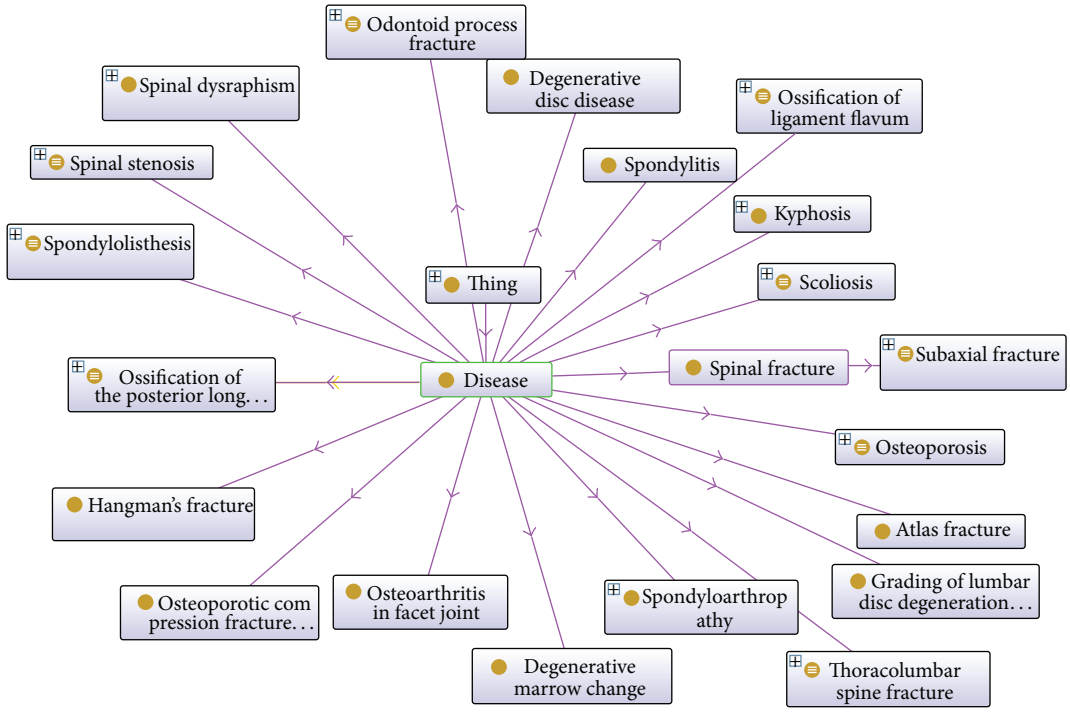


Figure 2: List of the spinal diseases shown in Protégé.

Figure 3: User interface of the proposed system.

model with OWL DL or Lite is needed. Further studies need to include the process of the transformation of literal object into resource object through the structuralization process of items completed by literal object, further systematizing the concept. In addition, the review of class and property is necessary to show the anatomical information of spine and information of diseases specifically. Also, the studies about methods which offer visual information are related to simulation model of KISTI.

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

References

[1] R. Mizoguchi, *The Next Generation Web and Critical Technology of Knowledge Processing*, Dooyangsa, 2009.

[2] R. Neches, R. Fikes, T. Finin et al., "Enabling technology for knowledge sharing," *AI Magazine*, vol. 12, no. 3, pp. 36–56, 1991.

[3] T. R. Gruber, "A translation approach to portable ontology specifications," *Knowledge Acquisition*, vol. 5, no. 2, pp. 199–220, 1993.

[4] J. H. Gennari, M. A. Musen, R. W. Fergerson et al., "The evolution of Protégé: an environment for knowledge-based systems development," *International Journal of Human Computer Studies*, vol. 58, no. 1, pp. 89–123, 2003.

[5] J. Ji, *Stedman's Medical Dictionary*, Koonja Publishing, 2006.

[6] Society TKSN, *The Textbook of Spine*, 2008.

[7] C. W. A. Pfirrmann, A. Metzdorf, M. Zanetti, J. Hodler, and N. Boos, "Magnetic resonance classification of lumbar intervertebral disc degeneration," *Spine*, vol. 26, no. 17, pp. 1873–1878, 2001.

[8] M. T. Modic and J. S. Ross, "Lumbar degenerative disk disease," *Radiology*, vol. 245, no. 1, pp. 43–61, 2007.

[9] S. Jeffrey, K. R. M. Ross, B. Bryson et al., *Diagnostic Imaging: Spine*, Amirsys, 2010.

[10] M. Pathria, D. J. Sartoris, and D. Resnick, "Osteoarthritis of the facet joints: accuracy of oblique radiographic assessment," *Radiology*, vol. 164, no. 1, pp. 227–230, 1987.

[11] D. Weishaupt, M. Zanetti, N. Boos, and J. Hodler, "MR imaging and CT in osteoarthritis of the lumbar facet joints," *Skeletal Radiology*, vol. 28, no. 4, pp. 215–219, 1999.

[12] J. W. M. van Goethem, L. van den Hauwe, P. Parizel, and A. L. Baert, *Spinal Imaging: Diagnostic Imaging of the Spine and Spinal Cord*, Springer, 2007.

Hindawi Publishing Corporation
Advances in Multimedia
Volume 2015, Article ID 575687, 9 pages
http://dx.doi.org/10.1155/2015/575687

Research Article

Performance Comparison of OpenMP, MPI, and MapReduce in Practical Problems

Sol Ji Kang, Sang Yeon Lee, and Keon Myung Lee

Department of Computer Science, Chungbuk National University, Cheongju, Chungbuk 361-763, Republic of Korea

Correspondence should be addressed to Keon Myung Lee; kmlee@cbnu.ac.kr

Received 29 August 2014; Accepted 8 November 2014

Academic Editor: Seungmin Rho

Copyright © 2015 Sol Ji Kang et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

With problem size and complexity increasing, several parallel and distributed programming models and frameworks have been developed to efficiently handle such problems. This paper briefly reviews the parallel computing models and describes three widely recognized parallel programming frameworks: OpenMP, MPI, and MapReduce. OpenMP is the de facto standard for parallel programming on shared memory systems. MPI is the de facto industry standard for distributed memory systems. MapReduce framework has become the de facto standard for large scale data-intensive applications. Qualitative pros and cons of each framework are known, but quantitative performance indexes help get a good picture of which framework to use for the applications. As benchmark problems to compare those frameworks, two problems are chosen: all-pairs-shortest-path problem and data join problem. This paper presents the parallel programs for the problems implemented on the three frameworks, respectively. It shows the experiment results on a cluster of computers. It also discusses which is the right tool for the jobs by analyzing the characteristics and performance of the paradigms.

1. Introduction

We often happen to meet problems requiring heavy computations or data-intensive processing. Hence, on one hand, we try to develop efficient algorithms for the problems. On the other hand, with the advances of hardware and parallel and distributed computing technology, we are interested in exploiting high performance computing resources to handle them.

Parallel and distributed computing technology has been focused on how to maximize inherent parallelism using multicore/many-core processors and networked computing resources [1–6]. Various computing architectures and hardware techniques have been developed such as symmetric multiprocessor (SMP) architecture, nonuniform memory access (NUMA) architecture, simultaneous multithreading (SMT) architecture, single instruction multiple data (SIMD) architecture, graphics processing unit (GPU), general purpose graphics processing unit (GPGPU), and superscalar processor [1, 7].

A variety of software technology has been developed to take advantage of hardware capability and to effectively develop parallel and distributed applications [2, 8]. With the plentiful frameworks of parallel and distributed computing, it would be of great help to have performance comparison studies for the frameworks we may consider.

This paper is concerned with performance studies of three parallel programming frameworks: OpenMP, MPI, and MapReduce. The comparative studies have been conducted for two problem sets: the all-pairs-shortest-path problem and a join problem for large data sets. OpenMP [9] is the de facto standard model from shared memory systems, MPI [10] is the de facto standard for distributed memory systems, and MapReduce [11] is recognized as the de facto standard framework intended for big data processing. For each problem, the parallel programs have been developed in terms of the three models, and their performance has been observed.

The remainder of the paper is organized as follows: Section 2 briefly reviews the parallel computing models and Section 3 presents the selected programming frameworks in more detail. Section 4 explains the developed parallel programs for the problems with the three frameworks.

Section 5 shows the experiment results and finally Section 6 draws conclusions.

2. Parallel Computing Models

In parallel computing memory architectures, there are shared memory, distributed memory, and hybrid shared-distributed memory [12]. Shared memory architectures allow all processors to access all memories as global memory space. They have usually been classified as uniform memory access (UMA) and NUMA. UMA machines are commonly referred to as SMP and assume all processors to be identical. NUMA machines are often organized by physically linking two or more SMPs in which not all processors have equal access time to all memories.

In distributed memory architectures, processors have their own memory, but there is no global address space across all processors. They have a communication network to connect processors' memories.

Hybrid shared-distributed memory employs both shared and distributed memory architectures. In clusters of multicore or many-core processors, cores in a processor share their memory and multiple shared memory machines are networked to move data from one machine to another.

There are several parallel programming models which allow users to specify concurrency and locality at a high level: thread, message passing, data parallel, and single program multiple data (SPMD) and multiple program multiple data (MPMD) models [12].

Thread model organizes a heavy weight process with multiple light weight threads that are executed concurrently. POSIX threads library (a.k.a. pthreads) [13] and OpenMP [9] are typical implementation of this model.

In the message passing model, an application consists of a set of tasks which use their own local memory that can be located in the same machine or across a certain number of machines. Tasks exchange data by sending and receiving messages to conduct the mission. MPI [10] is the de facto industry standard for message passing.

Data parallel model, also referred to as partitioned global address space (PGAS) model [14], provides each process with a view of the global memory even though memory is distributed across the machines. It makes distinction between local and global memory reference under the control of programmer. The compiler and runtime take care of converting remote memory access into message passing operations between processes [7]. There are several implementations of the data parallel model: Coarray Fortran, Unified Parallel C, X10, and Chapel [12].

SPMD model is a high level programming paradigm that executes the same program with different data multiple times. It is probably the most commonly used parallel programming model for clusters of nodes [12]. MPMD model is a high level programming paradigm that allows multiple programs to run on different data. With the advent of general purpose graphical processing unit (GPGPU), hybrid parallel computing models have been developed to utilize the many-core GPU to perform heavy computation under the control of the host thread running on the host CPU [15].

When data volume is large, demanding memory capacity may hinder its manipulation and processing. To deal with such situations, big data processing frameworks such as Hadoop and Dryad have been developed which exploit multiple distributed machines. Hadoop MapReduce is a programming model that abstracts an application into two phases of Map and Reduce [16]. Dryad structures the computation as a directed graph in which vertices correspond to a task and edges are the channels of data transmissions [17].

3. OpenMP, MPI, and MapReduce

3.1. OpenMP. OpenMP is a shared-memory multiprocessing application program inference (API) for easy development of shared memory parallel programs [9]. It provides a set of compiler directives to create threads, synchronize the operations, and manage the shared memory on top of pthreads. The programs using OpenMP are compiled into multithreaded programs, in which threads share the same memory address space and hence the communications between threads can be very efficient.

Compared to using pthreads and working with mutex and condition variables, OpenMP is much easier to use because the compiler takes care of transforming the sequential code into parallel code according to the directives [12]. Hence the programmers can write multithreaded programs without serious understanding of multithreading mechanism. Its runtime maintains the thread pool and provides a set of libraries [7].

It uses a block-structured approach to switch between sequential and parallel sections, which follows the fork/join model. At the entry of a parallel block, a single thread of control is split into some number of threads, and a new sequential thread is started when all the split threads have finished. Its directives allow the fine-grained control over the threads. It is supported on various platforms like UNIX, LINUX, and Windows and various languages like C, C++, and Fortran [12].

3.2. MPI. MPI is a message passing library specification which defines an extended message passing model for parallel, distributed programming on distributed computing environment [10]. It is not actually a specific implementation of the parallel programming environment, and its several implementations have been made such as OpenMPI, MPICH, and GridMPI [7]. In MPI model, each process has its own address space and communicates other processes to access others' address space. Programmers take charge of partitioning workload and mapping tasks about which tasks are to be computed by each process.

MPI provides point-to-point, collective, one-sided, and parallel I/O communication models [10]. Point-to-point communications enable exchanging data between two matched processes. Collective communication is a broadcast of message from a process to all the others. One-sided communications facilitate remote memory access without matched process on the remote node. Three one-sided libraries are available for remote read, remote write, and remote update [9]. MPI provides various library functions to

coordinate message passing in various modes like blocked and unblocked message passing. It can send messages of gigabytes size between processes.

MPI has been implemented on various platforms like Linux, OS X, Solaris, and Windows. Most MPI implementations use some kind of network file storage. As network file storage, network file system (NFS) and Hadoop HDFS can be used. Because MPI is a high level abstraction for parallel programming, programmers can easily construct parallel and distributed processing applications without deep understanding of the underlying mechanism of process creation and synchronization. To order to exploit the multicore of processors, the MPI processes can be organized to have multiple threads in themselves. MPI-based programs can be executed on a single computer or a cluster of computers [18].

3.3. MapReduce. MapReduce is a programming paradigm to use Hadoop which is recognized as a representative big data processing framework [11]. Hadoop clusters consist of up to thousands of commodity computers and provide a distributed file system called HDFS which can accommodate big volume of data in a fault-tolerant way [19]. The clusters become the computing resource to facilitate big data processing [20, 21].

MapReduce organizes an application into a pair (or a sequence of pairs) of Map and Reduce functions. It assumes that input for the functions comes from HDFS file(s) and output is saved into HDFS files. Data files consist of records, each of which can be treated as a key-value pair. Input data is partitioned and processed by Map processes, and their processing results are shaped into key-value pairs and shuffled into Reduce tasks according to key. Map processes are independent of each other and thus they can be executed in parallel without collaboration among them. Reduce processes play role of aggregating the values with the same key.

MapReduce runtime launches Map and Reduce processes with consideration of data locality. The programmers do not have to consider data partitioning, process creation, and synchronization. The same Map and Reduce functions are executed across machines. Hence, MapReduce paradigm can be regarded as a kind of SPMD model.

MapReduce paradigm is a good choice for big data processing because MapReduce handles data record by record without loading whole data into memory and in addition the program is executed in parallel over a cluster [20]. It is very convenient to develop big data handling programs using MapReduce because Hadoop provides everything needed for distributed and parallel processing behind the scene which program does not need to know.

4. Parallel Programs for the All-Pairs-Shortest-Path Problem and a Join Problem

This paper is concerned with comparative performance studies of OpenMP, MPI, and MapReduce. OpenMP and MPI have been compared earlier in [3, 22], but they have not been usually compared with MapReduce because MapReduce does not assume any special memory architecture. With increasing interest in big data, many practitioners are interested in using MapReduce to handle big volume of data and sometimes computation-intensive problems [20].

Once you understand their design principle and underlying mechanism of the frameworks, you might guess which seems to be better in which situation. This study is intended to get quantitative figures about their performance. Here we choose as benchmark problems two problems: the all-pairs-shortest-path problem as a computation-intensive one and a join problem as a data-intensive one.

$n \leftarrow$ size of rows
$D^{(0)} \leftarrow$ input distance matrix
$\Pi^{(0)} \leftarrow$ calculate precedence matrix
for $k \leftarrow 1$ to n
  do for $i \leftarrow 1$ to n
    do for $j \leftarrow 1$ to n
      do $d_{ij}^{(k)} \leftarrow \min\left(d_{ij}^{(k-1)}, d_{ik}^{(k-1)} + d_{kj}^{(k-1)}\right)$

$$\pi_{ij}^{(k)} = \begin{cases} \pi_{ij}^{(k-1)} & \text{if } d_{ij}^{(k-1)} \leq d_{ik}^{(k-1)} + d_{kj}^{(k-1)} \\ \pi_{kj}^{(k-1)} & \text{if } d_{ij}^{(k-1)} > d_{ik}^{(k-1)} + d_{kj}^{(k-1)} \end{cases}$$

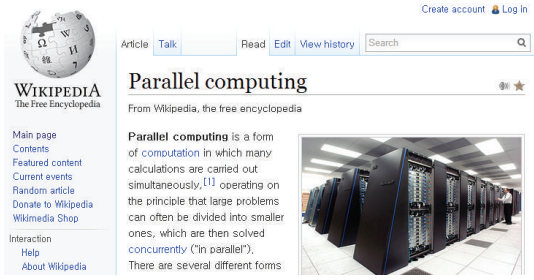
return $D^{(n)}$ and $\Pi^{(n)}$

Algorithm 1: Floyd-Warshall algorithm for the all-pairs-shortest-path problem.

4.1. Benchmark Problems. The all-pairs-shortest-path problem is to find the shortest path between all pairs of nodes in a graph. The problem occurs in domains of communication networking, logistics planning, layout design, navigation, and so on. Floyd-Warshall algorithm is one of the best known algorithms to this problem, which iteratively searches the shortest paths by considering the intermediate nodes one by one [23]. Algorithm 1 shows Floyd-Warshall algorithm, where $D = (d_{ij})$ denotes the matrix containing the distance d_{ij} between nodes i and j, $\Pi = (\pi_{ij})$ is the precedence matrix containing the information about the shortest paths between nodes, $d_{ij}^{(k)}$ is the distance found which is obtained by using the node set $\{1, 2, \ldots, k\}$ as intermediate nodes, and $\pi_{ij}^{(k)}$ is the predecessor of node j on the shortest path from node i to j obtained by using the node set $\{1, 2, \ldots, k\}$ as intermediate nodes.

As the second benchmark problem, we choose the task to find associated English Wikipedia pages with English keywords appearing in Korean Wikipedia pages and then place the hyperlinks from the English words of Korean Wikipedia pages to the found English Wikipedia pages. Wikipedia is a free-access Internet encyclopedia which has 287 language editions (as of August 2014). Figure 1(a) shows the Korean Wikipedia page for the word "parallel computing" of which content is mostly written in Korean and some notable terms like "parallel computing" are put into the parenthesis in English. Figure 1(b) shows the corresponding English Wikipedia page for the term "parallel computing." We want to place a hyperlink from the word "parallel computing" of the page of Figure 1(a) to the page of Figure 1(b).

(a)



(b)

Figure 1: A join problem to insert a hyperlink from English words "parallel computing" of Korean Wikipedia pages to the corresponding page of English Wikipedia. (a) Korean Wikipedia (http://ko.wikipedia.com/) and (b) English Wikipedia (http://en.wikipedia.com/).

The hyperlink construction problem can be regarded as a join problem: Korean Wikipedia pages are reviewed as a table of the pairs of English word(s) and the corresponding page contents, and English pages are also reviewed as a table of the pairs of their title and their URL. The inner join between two tables gives all needed information for hyperlink construction. In the benchmark problem, we have an English Wikipedia XML archive with 4,664,819 articles of size 4.04 gigabytes and a Korean Wikipedia XML archive with 529,997 articles of size 1.35 gigabytes. Hence the problem is data-intensive one to deal with large volume of data.

4.2. Distributed Programs for the All-Pairs-Shortest-Path Problem. To compare the performance of OpenMP, MPI, and MapReduce models for the all-pairs-shortest-path problem, the distributed programs are developed based on each model as follows. All the programs in fact implement the Floyd-Warshall algorithm in parallel executing codes.

Algorithm 2 shows the pseudocode for solving the all-pairs-shortest-path problem which is based on the OpenMP. In the code, "parallel start" indicates the parallel execution directive which spawns a team of threads as needed to take care of the loop in a partitioned manner. "Parallel end" indicates the place at which all threads join together into a single thread.

Algorithm 3 shows the MPI-based pseudocode for the all-pairs-shortest-path problem. In the code, "MPI Init" indicates the place to load and initialize the MPI library, and "MPI Finalize" is the part to wrap up the MPI processing. According to the process ID "pid," each process takes care

$n \leftarrow$ size of rows
$D^{(0)} \leftarrow$ input distance matrix
$\Pi^{(0)} \leftarrow$ calculate precedence matrix
tN $\leftarrow$ number of threads
for $k \leftarrow 1$ to n
  parallel start
    tid $\leftarrow$ id of thread
    for $i \leftarrow \dfrac{\text{tid} * n}{\text{tN}}$ to $\dfrac{(\text{tid}+1) * n}{\text{tN}} - 1$
      for $j \leftarrow 1$ to n

$$d_{ij}^{(k)} \leftarrow \min\left(d_{ij}^{(k-1)}, d_{ik}^{(k-1)} + d_{kj}^{(k-1)}\right)$$

$$\pi_{ij}^{(k)} = \begin{cases} \pi_{ij}^{(k-1)} & \text{if } d_{ij}^{(k-1)} \le d_{ik}^{(k-1)} + d_{kj}^{(k-1)} \\ \pi_{kj}^{(k-1)} & \text{if } d_{ij}^{(k-1)} > d_{ik}^{(k-1)} + d_{kj}^{(k-1)} \end{cases}$$

  parallel end
return $D^{(n)}$ $\Pi^{(n)}$

Algorithm 2: OpenMP pseudocode for the all-pairs-shortest-path problem.

MPI Init
$n \leftarrow$ size of rows
pid $\leftarrow$ id of process
pN $\leftarrow$ number of processes
$D^{(0)} \leftarrow$ input distance matrix
$\Pi^{(0)} \leftarrow$ calculate precedence matrix
for $k \leftarrow 1$ to n
  do for $i \leftarrow \dfrac{\text{pid} * n}{\text{pN}}$ to n
    do for $j \leftarrow 1$ to n
      do

$$d_{ij}^{(k)} \leftarrow \min\left(d_{ij}^{(k-1)}, d_{ik}^{(k-1)} + d_{kj}^{(k-1)}\right)$$

$$\pi_{ij}^{(k)} = \begin{cases} \pi_{ij}^{(k-1)} & \text{if } d_{dj}^{(k-1)} \le d_{ik}^{(k-1)} + d_{kj}^{(k-1)} \\ \pi_{kj}^{(k-1)} & \text{if } d_{ij}^{(k-1)} > d_{ik}^{(k-1)} + d_{kj}^{(k-1)} \end{cases}$$

    send i'st row to another processes
    receive updated rows from another processes
return $D^{(n)}$ $\Pi^{(n)}$
MPI Finalize

Algorithm 3: MPI pseudocode for the all-pairs-shortest-path problem.

of the assigned part and sends and receives the intermediate results to and from other processes.

Algorithm 4 shows the pseudocode based on MapReduce model. MapReduce model abstracts the job with Map and Reduce functions. Map function is applied to each record of the input file where a line contains a record. Reduce function takes the whole outputs of Map function and aggregates them into final results. The implemented application iteratively repeats these MapReduce phases as many as the number of nodes in the input graph. In the code, "Driver( )" plays the role of a coordinate to invoke MapReduce cycles iteratively. An input record [key = $(i \;\; j)$, val = $(d_{ij}^{(k-1)} \;\; \pi_{ij}^{(k-1)})$] of Map function means that the so far shortest distance from node i to j is $d_{ij}^{(k-1)}$ and the preceding node of node j in the shortest path is $\pi_{ij}^{(k-1)}$, and "write($i \;\; j, \;\; i \;\; j \;\; d_{ij}^{(k-1)} \;\; \pi_{ij}^{(k-1)}$)" indicates

input: $\left[i \quad j \quad d_{ij}^{(k-1)} \quad \pi_{ij}^{(k-1)}\right]$
Map(Object key = $(i \quad j)$, Value val = $\left(d_{ij}^{(k-1)} \quad \pi_{ij}^{(k-1)}\right)$)
  if $i == k$ or $j == k$ then
    for $m \leftarrow 1$ to n
      if $j == k$ then write$(j \quad m), \left(i \quad j \quad d_{ij}^{(k-1)} \quad \pi_{ij}^{(k-1)}\right)$
      if $i == k$ then write$(m \quad i), \left(i \quad j \quad d_{ij}^{(k-1)} \quad \pi_{ij}^{(k-1)}\right)$
    else then write$(i \quad j), \left(i \quad j \quad d_{ij}^{(k-1)} \quad \pi_{ij}^{(k-1)}\right)$
Reduce(Object key = $(i \quad j)$, Value val = $\left(i \quad j \quad d_{ij}^{(k-1)} \quad \pi_{ij}^{(k-1)}\right)$)
  $d_{ij}^{(k)} \leftarrow \min\left(d_{ij}^{(k-1)}, d_{ik}^{(k-1)} + d_{kj}^{(k-1)}\right)$
  $\pi_{ij}^{(k)} = \begin{cases} \pi_{ij}^{(k-1)} \text{ if } d_{ij}^{(k-1)} \leq d_{ik}^{(k-1)} + d_{kj}^{(k-1)} \\ \pi_{kj}^{(k-1)} \text{ if } d_{ij}^{(k-1)} > d_{ik}^{(k-1)} + d_{kj}^{(k-1)} \end{cases}$
  write$(i \quad j), \left(d_{ij}^{(k)} \quad \pi_{ij}^{(k)}\right)$
Driver( )
  $n \leftarrow$ size of rows
  for $k \leftarrow 1$ to n
    Map$\left((i \quad j), \left(d_{ij}^{(k-1)} \quad \pi_{ij}^{(k-1)}\right)\right)$
    Reduce$\left((i \quad j), \left(i \quad j \quad d_{ij}^{(k-1)} \quad \pi_{ij}^{(k-1)}\right)\right)$

Algorithm 4: MapReduce pseudocode for the all-pairs-shortest-path problem.

the operation to write out a record with key $(i \quad j)$ and value $(i \quad j \quad d_{ij}^{(k-1)} \quad \pi_{ij}^{(k-1)})$ to a HDFS file.

4.3. Distributed Programs for the Join Problem. In the join problem, there are two XML files: a Korean Wikipedia XML file and an English Wikipedia file. First, we need to extract the English terms from Korean Wikipedia file and create a table of records, each of which consists of English term(s) and the original page content for the later use. The English Wikipedia file is transformed into a table of records consisting of the page title and the page URL. After that, the two tables are joined to obtain the information about hyperlinks to be added.

Algorithm 5 shows the pseudocode for the join problem to obtain the hyperlink information by using the OpenMP construct. The two files are too large to be fit into the main memory. Hence, they are partitioned and the larger file (i.e., English Wikipedia file) is sequentially read into the memory one by one just once, and the partitions of the smaller file are read sequentially as many as the number of partitions of the larger files.

Algorithm 6 shows the MPI pseudocode for the join problem. In the code, "send" and "receive" denote the MPI communication APIs for data exchange. Each process takes care of the partitioned job and files are read line by line which is supported for large volume of data by the operating system like Linux.

Algorithm 7 shows the MapReduce codes of two Map functions for both Korean Wikipedia articles and English Wikipedia articles and a Reduce function. The Korean Wikipedia Map function extracts English word(s) from each Korean page and produces records of word(s) and the entire article. The English Wikipedia Map function extracts the title and URL of an English page and generates a record with them. The Reduce function receives the outputs of both Maps and finds matched pairs to build the information of hyperlinks from words in Korean pages to English pages. Figure 2 shows the configuration of Map and Reduce functions to extract the hyperlink information from the two files.

5. Experiments

For the two benchmark problems, the parallel programs have been implemented using OpenMP, MPI, and MapReduce, respectively. In the experiments, a cluster of 5 PCs was used, each of which has Intel Core i7-4770 3.40 GHz CPU and 16 GB RAM, and was installed with CentOS-6.4 LINUX 64 bits. For MapReduce applications, Hadoop HDFS and YARN were installed over the cluster where HDFS is the distributed file system in Hadoop and YARN is a resource and application manager. MPICH, which is an implementation of MPI, was installed at each machine on YARN and HDFS. OpenMP was installed on a single node because it supports only shared memory model but not distributed memory model.

For the all-pairs-shortest-path problem, three sample graphs were randomly generated of which the numbers of nodes were 10, 100, and 1000, respectively. When they were generated, each node was set to be linked to half of the other nodes. When final results are written, there can exist a bottleneck if a single file is used as the output. Hence, for the fair comparisons, each process or thread is allowed to write its output into its own out-file.

Table 1 shows the execution time obtained in the all-pairs-shortest-path problem experiments. For this computation-intensive problem, the OpenMP program gave the best performance where 10 threads were used. The MPI program was executed on a single machine and on the cluster of 5 machines with total of 10 processes. Due to the computational

```
OMP_JOIN_PAGE(char* koFile, char* enFile, char* outFile)
  tN ← number of threads
  eS ← block size of English Wikipedia file to be read at a time
  eN ← number of blocks in English Wikipedia file, enFile
  kS ← block size of Korean Wikipedia file to be read at a time
  kN ← number of blocks in Korean Wikipedia file, koFile
  for i ← 1 to eN
    eBlock ← ith block of enFile
    for k ← 1 to kN
      kBlock ← kth block of koFile
      parallel-start
        tid ← id of thread
        for j ← (tid * eS)/tN to ((tid + 1) * eS)/tN − 1
          text ← eBlock.nextLine()
          title ← searchTitle(text)
          url ← searchUrl(text)
          foreach text ∈ kBlock
            content ← searchContent(text)
            koUrl ← searchUrl(text)
            wordList[] ← extractEngKeyword(content)
            foreach word ∈ wordList[] do
              if isMatched(word, title) then
                enUrl ← url
              else
                enUrl ← φ
              if enUrl ≠ φ
                write(title, koUrl, word, enUrl)
      parallel-end
```

Algorithm 5: OpenMP pseudocode for the join problem.

Table 1: Execution times for the all-pairs-shortest-path problem.

Node size	Framework			
	MapReduce	MPI		OpenMP
		Cluster	Single machine	
10	2 m 26 s	0.32 s	0.34 s	0.1 s
100	16 m 52 s	0.44 s	0.41 s	0.25 s
1000	4 h 4 m 39 s	4 m 48 s	24.14 s	8.03 s

Table 2: Execution time for the join problem.

Problem	Framework		
	MapReduce	MPI	OpenMP
The join problem	24 m 15 s	135 h 34 m	93 h 14 m

overhead, the cluster showed poor performance for the MPI program. In the experiment setting, the communication bottleneck was severe even though the machines were connected with a 1 Gbps switching hub. The performance of MPI on a single machine is not comparable to OpenMP, because OpenMP threads share the global address space but MPI processes communicate using the message passing protocol. If some application can be run on a high-end single machine, OpenMP is preferred to MPI. MapReduce is not a choice for computational-intensive and iterative computation problems like the all-pairs-shortest-path problem.

Table 2 shows the experiment results for the join problem. The execution time varies depending on the execution context like network bandwidth and resource management of operating systems, hence the same experiments have been conducted three times for each setting. For fair comparisons, no special indexing structures like B+ tree [23] were used in implementing the join operations. However, the same logic was implemented on each framework. The MapReduce-based program was the best one among the three models. In the join operation, we need only the title and URL of English Wikipedia pages and hence the implementations of MPI and OpenMP just scan the English pages as a stream and keep the whole set of the pairs of the title and the URL in the memory. Then, Korean Wikipedia pages are read one by one in order to examine which English terms appear. OpenMP gave better performance than MPI for the join problem because the curated information for English pages was loaded into the memory in a whole, and OpenMP threads have no communication overhead to access the memory. From these observations, we see that MapReduce is the best choice for data-intensive processing of big volume of data.

```
MPI_JOIN_PAGES(char* koFile, char* enFile, char* outFile)
  koFileLineSize ← getFileLines(koFile)
  MPI-Init
  nRank ← process ID number within communicator
  divLine ← the number of each process's allocated lines
  line ← move file pointer to the first of allocated lines
  if nRank = 0 then
    while true do
      send (NULL, NULL, NULL, NULL, true)
        to another processes
      receive (title, koUrl, word, enUrl, isLast)
        from another processes
      out.Write(title, koUrl, word, enUrl)
      if isLast(ALL) then break
  else
    for i = 0 to divLine do
      text ← enFile.nextLine(line + i)
      title ← searchTitle(text)
      content ← searchContent(text)
      koUrl ← searchUrl(text)
      wordList[] ← extractEngKeyword(content)
      foreach word ∈ wordList[] do
        if isExist(word, enFile) then
          enUrl ← getUrl(word, enFile)
        else
          enUrl ← φ
        send (title, koUrl, word, enUrl, isLast)
          to another processes
        receive (title, koUrl, word, enUrl, isLast)
          from another processes
      if isLast(ALL) then break
  MPI-Finalize
```

Algorithm 6: MPI pseudocode for the join problem.

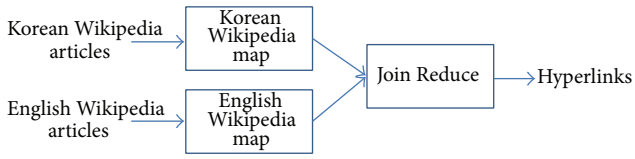


Figure 2: MapReduce pseudocode for the join problem.

6. Conclusions

OpenMP, MPI, and MapReduce are the most widely recognized parallel or distributed programming frameworks. Each one is said to be the de facto standard on its computing model. To evaluate their performance, we implemented the programs for both the all-pairs-shortest-path problem and the join problem for hyperlink extraction from two files using the three frameworks, respectively. The performance of each model was measured in terms of the execution time.

From the experiment results, we observed the following things. If a problem is small enough to be accommodated and the computing resources such as cores and memory are sufficient, OpenMP is a good choice. When data size is moderate and the problem is computation-intensive, MPI can be considered the framework. When data size is large and the tasks do not require iterative processing, MapReduce can be an excellent framework. OpenMP is the easiest to use because there is no special attention needed to be paid because we just need to place some directives in the sequential code. MapReduce is relatively easy to use once we can abstract an application into Map and Reduce steps. The programmers do not have to consider workload partitioning and synchronization. MapReduce programs, however, take considerable time for the problems requiring much iteration, like all-pairs-shortest-path problem. MPI allows more flexible control structures than MapReduce; hence MPI is a good choice when a program is needed to be executed in parallel and distributed manner with complicated coordination among processes.

This study did not consider the CUDA (compute unified device architecture) model which is a parallel computing platform and programming model for GPUs [24]. It would be interesting to compare CUDA with the discussed programming models for some additional practical problem sets.

```
MAP for Korean Wikipedia:
  Input Korean Wikipedia XML File
  MAP(Object key = null, Page input = Korean Wikipedia file)
    line ← input.readLine()
    title ← searchTitle(line)
    content ← searchContent(line)
    wordList[] ← extractEngKeyword(content)
    for all word ∈ wordList[] do
      write(word, input)
MAP for English Wikipedia File
  Input: English Wikipedia XML File
  MAP(Object key = null, Page input = English Wikipedia file)
    line ← input.readLine()
    title ← searchTitle(line)
    url ← searchUrl(line)
    Page out(title:title, url:url)
    write(title, out)
REDUCE(Text key, Page [p1, p2, ...])
  word ← ∅
  url ← ∅
  list ← new List<Page>
  for all p ∈ [p1, p2, ...] do
    if IsEnglish(p) then
      word ← p.getTitle()
      url ← p.getUrl()
    else
      list.add(p)
  for all koreanPage ∈ list do
    koreanPage.setWord(word)
    koreanPage.setUrl(url)
    write(key, koreanPage)
```

Algorithm 7: MapReduce pseudocode for the join problem.

Conflict of Interests

No potential conflict of interests relevant to this paper was reported.

Acknowledgment

This research was supported by the MSIP (Ministry of Science, ICT and Future Planning), Korea, under the ITRC (Information Technology Research Center) support Program (NIPA-2013-H0301-13-4009) supervised by the NIPA (National IT Industry Promotion Agency).

References

[1] D. E. Culler, J. P. Singh, and A. Gupta, *Parallel Computer Architecture: A Hardware/software Approach*, Gulf Professional, 1999.

[2] A. C. Sodan, "Message-passing and shared-data programming models—wish vs. reality," in *Proceedings of the 19th International Symposium on High Performance Computing Systems and Applications (HPCS '05)*, pp. 131–139, May 2005.

[3] K. M. Lee and K. M. Lee, "Similar pair identification using locality-sensitive hashing technique," in *Proceedings of 6th International Conference on Soft Computing and Intelligent Systems, and 13th International Symposium on Advanced Intelligence Systems (SCIS/ISIS '12)*, pp. 2117–2119, 2012.

[4] H. Lee-Kwang, K. A. Seong, and K. M. Lee, "Hierarchical partition of nonstructured concurrent systems," *IEEE Transactions on Systems, Man, and Cybernetics Part B: Cybernetics*, vol. 27, no. 1, pp. 105–108, 1997.

[5] S. W. Lee, J. T. Kim, H. Wang et al., "Architecture of RETE network hardware accelerator for real-time context-aware system," *Lecture Notes in Computer Science*, vol. 4251, pp. 401–408, 2006.

[6] S. W. Lee, J. T. Kim, B. K. Sohn, K. M. Lee, J. W. Jeon, and S. Lee, *Real-Time System-on-a-Chip Architecture for Rule-Based Context-Aware Computing*, vol. 3681 of *Lecture Notes in Computer Science*, 2005.

[7] J. Diaz, C. Muñoz-Caro, and A. Niño, "A survey of parallel programming models and tools in the multi and many-core era," *IEEE Transactions on Parallel and Distributed Systems*, vol. 23, no. 8, pp. 1369–1386, 2012.

[8] S. C. Ravela, "Comparison of shared memory based parallel programming models," Tech. Rep. MSC-2010-01, Blekinge Institute of Technology, 2010.

[9] OpenMP Architecture Review Board, "OpenMP Application Program Interface," 2008, http://www.openmp.org/mp-documents/spec30.pdf.

[10] W. Gropp, S. Huss-Lederman, A. Lumsdaine et al., *MPI: The Complete Reference, the MPI-2 Extensions*, vol. 2, The MIT Press, 1998.

[11] J. Dean and S. Ghemawat, "MapReduce: simplified data processing on large clusters," *Communications of the ACM*, vol. 51, no. 1, pp. 107–113, 2008.

[12] B. Barney, *Introduction to Parallel Computing*, Lawrence Livermore National Laboratory, 2007, https://computing.llnl.gov/tutorials/parallel_comp/.

[13] POSIX-IEEE Standards Association, 2014, http://standards.ieee.org/develop/wg/POSIX.html.

[14] C. Coarfa, Y. Dotsenko, J. Mellor-Crummey et al., "An evaluation of global address space languages: co-array fortran and Unified Parallel C," in *Proceedings of the 10th ACM SIGPLAN Symposium on Principles and Practise of Parallel Programming*, pp. 36–47, June 2005.

[15] M. Macedonia, "The GPU enters computing's mainstream," *Computer*, vol. 36, no. 10, pp. 106–108, 2003.

[16] A. Alexandrov, S. Ewen, M. Heimel et al., "MapReduce and PACT—comparing data parallel programming models," in *Proceedings of the 14th Conference on Database Systems for Business, Technology, and Web (BTW '11)*, pp. 25–44, 2011.

[17] M. Isard, M. Budiu, Y. Yu, A. Birrell, and D. Feterly, "Dryad: distributed data-parallel programs from sequential building blocks," *ACM SIGOPS Operating Systems Review*, vol. 41, no. 3, pp. 59–72, 2007.

[18] G. Jost, H. Jin, D. Mey, and F. Hatay, "Comparing the OpenMP, MPI, and hybrid programming paradigm on an SMP cluster," in *Proceedings of the 5th European workshop on OpenMP (EWOMP '03)*, 2003.

[19] S. Ghemawat, H. Gobioff, and S.-T. Leung, "The google file system," in *Proceedings of the 19th ACM Symposium on Operating Systems Principles (SOSP '03)*, pp. 29–43, October 2003.

[20] C. Ranger, R. Raghuraman, A. Penmetsa, G. Bradski, and C. Kozyrakis, "Evaluating MapReduce for multi-core and multiprocessor systems," in *Proceedings of the 13th IEEE International Symposium on High Performance Computer Architecture (HPCA '07)*, pp. 13–24, Scottsdale, Ariz, USA, February 2007.

[21] S. J. Plimpton and K. D. Devine, "MapReduce in MPI for large-scale graph algorithms," *Parallel Computing*, vol. 37, no. 9, pp. 610–632, 2011.

[22] M. Resch, B. Sander, and I. Loebich, "A comparison of OpenMP and MPI for the parallel CFD test case," in *Proceedings of the 1st European Workshop on OpenMP*, pp. 71–75, 1999.

[23] T. H. Cormen, C. E. Leiserson, R. L. Rivest, and C. Stein, *Introduction to Algorithms*, MIT Press, 2009.

[24] J. Nickolls, I. Buck, M. Garland, and K. Skadron, "Scalable parallel programming with CUDA," *Queue*, vol. 6, no. 2, pp. 40–53, 2008.

Hindawi Publishing Corporation
Advances in Multimedia
Volume 2015, Article ID 468128, 8 pages
http://dx.doi.org/10.1155/2015/468128

Research Article

Coevolution of Artificial Agents Using Evolutionary Computation in Bargaining Game

Sangwook Lee

School of Information & Communication Convergence Engineering, College of Engineering, Mokwon University, Room D506, 88 Doanbuk-ro, Seo-gu, Daejeon 302-318, Republic of Korea

Correspondence should be addressed to Sangwook Lee; slee@mokwon.ac.kr

Received 29 August 2014; Accepted 23 October 2014

Academic Editor: Seungmin Rho

Copyright © 2015 Sangwook Lee. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Analysis of bargaining game using evolutionary computation is essential issue in the field of game theory. This paper investigates the interaction and coevolutionary process among heterogeneous artificial agents using evolutionary computation (EC) in the bargaining game. In particular, the game performance with regard to payoff through the interaction and coevolution of agents is studied. We present three kinds of EC based agents (EC-agent) participating in the bargaining game: genetic algorithm (GA), particle swarm optimization (PSO), and differential evolution (DE). The agents' performance with regard to changing condition is compared. From the simulation results it is found that the PSO-agent is superior to the other agents.

1. Introduction

The current bargaining game research is based on the established theoretical model of Ståhl [1] and Rubinstein [2]. Game theorists, economists, psychologists, and computer scientists have already started analyzing the underlying bargaining phenomenon which can be applied in e-commerce application [3], negotiation problem [4], and dispute resolution [5], to name a few. The game appears to be very simple but the results are fuzzy and controversial.

Over the past few years, a considerable number of studies have been conducted on modeling the bargaining game using artificial agents on the interaction among the homogeneous population. However, very few attempts have been made at the study on the interaction among the heterogeneous population. Matwin et al. designed a negotiation support system (NSS) which addresses multiple issues through populations of rules (classifier) which are learned by means of GA thereby supporting a two-party bargaining game [6]. Meanwhile, using evolution strategy, Page et al. proposed a generalized adaptive dynamic framework that can deal with games in which the payoff is not differentiable [7]. van Bragt and La Poutrè formulated bargaining strategies as finite automata coevolved by genetic algorithm to discriminate different opponents without any information about the identity or preferences of their counterparts [8]. Takadama et al. suggested three learning bargaining models which are based on evolution strategy (ES), learning classifier system (LCS), and reinforcement learning (RL) strategy. They evaluated heterogeneous-population interactions in their study [9]. Zhong et al. have tried to show that artificial agents with RL strategy can evolve against fixed rules and rotating rules with better performance [10]. Cooper et al. further utilized the RL strategy in terms of observing the relative speeds of learning by proponents and respondents [11]. Grosskopf studied the combined effect of RL and directional learning (DL) strategy in order to compare the result of the one-shot bargaining game with a proponent and varying respondents and showed that the strategies can coevolve [12].

The above studies have focused on the validity of the artificial agent models and compared the results of homogeneous-population interactions. However, these studies on the homogeneous-population interactions are conservative approaches due to the reason that the real-world bargaining game aims at the analysis of the deal in which there exist many behaviors with diversified propensities and tendencies, characterizing many kinds of agents.

In this paper we proceed to study interactions of agents in the heterogeneous population. We conducted experiments with three kinds of evolutionary computation based agents to play the bargaining game. From the experiments we identify what are the principal parameters and how much they affect the results of the bargaining game. Also patterns of action of artificial agents are analyzed according to their strategy. In particular, a bargaining game among EC-agents was conducted to observe the interaction and coevolution.

This paper is organized as follows: Section 2 briefly reviews the sequential bargaining game. The next section outlines the design consideration of artificial agents. In Section 4, coevolution model among EC-agents is described. The simulation results are demonstrated in Section 5. Finally, the paper concludes with some remarks in Section 6.

2. Sequential Bargaining Game

The sequential bargaining game is a division game of a fixed sum between two players. There exist infinite number of Nash equilibriums in the bargaining game according to the game theory and the subgame perfect equilibrium is that the last proponent makes a proposal as the ε, the lowest nonzero quantity, to the counterpart and the respondent always accepts the minimal proposal since any ε is better than a null demand. But experimental evidence is in contrast with this strategy due to the fact that the proponents tend to offer the counterpart more than the noncooperative game theory predicts, and the respondents reject the small offers. The rejection of a low offer by the respondent can be seen as punishment. Page et al. surveyed that "some 60~80% of proponents offer fractions between 0.4 and 0.5, and only 3% offer less than 0.2. They are well advised to do this—indeed, some 50% of respondents reject any split offering them less than one-third of the sum" [7, 13–15]. It seems discrepancy between game theory and experimental data results from the notion of fairness and the absence of common knowledge of rationality [16–18]. Recently, extensive studies have been carried out on the analysis of the bargaining game through the use of artificial agents [19–21].

A brief review, in this respect, follows. However, before that we prefer to review the following terms for clarity.

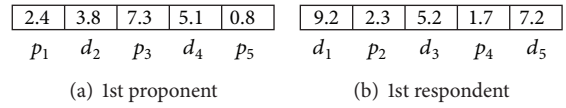
(i) Payoff: reward which agent receives from the game.

(ii) Control parameter: EC-agents factor which can affect the performance of agent in game.

(iii) Sequential game: the game composed of multiple rounds.

3. Artificial Agent Models

In this section, we discuss the underlying bargaining game phenomenon vis-à-vis simulation models. The game kicks off by virtue of randomly, that is, with equal probability, deciding a proponent and a respondent. The proponent chooses a proposal p_k, a real number between 0 and 10, which is the amount the proponent is able to pay at round k. The respondent chooses a minimal acceptable demand d_k, which is also a real number between 0 and 10 at round k. If the proposal is more than the demand, that is, if $p_k \geq d_k$, then the proponent earns $10 - p_k$, and the respondent earns p_t. If the proposal is not accepted, that is, if $p_k < d_k$, then the status of two players is exchanged and set at round $k = k+1$. Finally if the deal between the two players is failed in the last round, that is, $k = 5$ in our experiment, then each player earns null.



(a) 1st proponent (b) 1st respondent

Figure 1: Representation of solution.

We introduce three kinds of the artificial agents for evolving strategies using genetic algorithms (GA), particle swarm optimization (PSO), and differential evolution (DE). These ECs are based on an arbitrarily initialized population of trial solution which evolves toward better solution by means of each EC operators.

Figure 1 shows an EC-agent which is called solution, strategy, vector, and position. In a bargaining game, it is important whether the gamer begins the first transaction as a proponent or a respondent, and thus each strategy is composed of two vectors. The first vector represents a strategy to put an EC-agent in the first proponent position and the second in the first respondent position. When the agent is the first proponent, the first row is used as its strategy, otherwise, the second row.

3.1. GA-Agent Model. Genetic algorithm (GA) is a search algorithm based on the mechanics of natural system, that is, the law of the survival of the fittest [22]. GA operators consist of selection, crossover, and mutation. Fitness value of individual solutions is measured by a payoff which a GA-agent earns in the bargaining game.

In GA-agent, we use a tournament selection, arithmetic crossover, and mutation as GA operators. The tournament selection is a selection method that one picks up two solutions randomly from current population and chooses a winner between them [23]. The arithmetic crossover is a crossover method that each gene of offspring is averaged value of two parents' genes. As for mutation, we use the method to initialize genes. Figure 2 shows an evolution process of GA-agent.

3.2. PSO-Agent Model. Particle swarm optimization (PSO) is a metaheuristic method that optimizes a problem by iteratively trying to improve a candidate solution by moving particles, which are candidate solutions, around in the search space according to simple mathematical formulae which are concerned with particle's position update and velocity update [24]. Each particle's movement is influenced by its local best known position but is also guided toward the best known positions in the search space, which are updated as better positions found by other particles.

The PSO algorithm is initialized with the population of individuals being placed randomly on the search space and searching for an optimal solution by updating individual

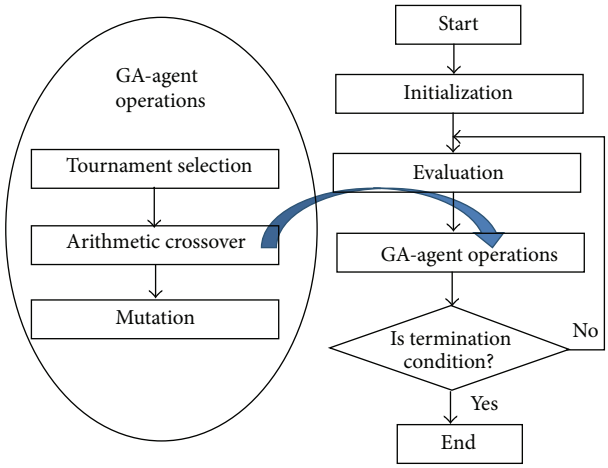


Figure 2: Evolution process of a GA-agent.

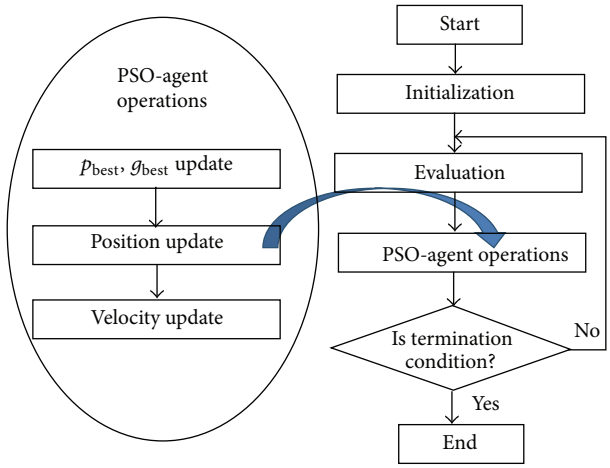


Figure 3: Evolution process of a PSO-agent.

generations. In each iteration, the velocity and the position of each particle are updated according to its previous best position ($p_{\text{best},i,j}$) and the best position found by neighbors of the particle ($g_{\text{best},i,j}$). The formula of particle's velocity and position update is as follows:

$$v_{i,j}(t+1) = wv_{i,j}(t) + c_1R_1\left(p_{\text{best},i,j} - x_{i,j}(t)\right) + c_2R_2\left(g_{\text{best},i,j} - x_{i,j}(t)\right), \quad (1)$$
$$x_{i,j}(t+1) = x_{i,j}(t) + v_{i,j}(t+1),$$

where i is the index of particles in the swarm, j is the index of positions in the particle, t represents the iteration number, $v_{i,j}(t)$ is the velocity vector of the ith particle, and $x_{i,j}(t)$ is the position vector. Note that c_1 and c_2 are the positive acceleration constants, R_1 and R_2 are random numbers uniformly distributed between 0 and 1, and w is the inertia weight.

In [25], it was shown that a good convergence can be ensured by making two constants which are an acceleration and inertia. This can be demonstrated from the relation between them using an intermediate parameter φ. Consider the following:

$$w = \frac{1}{\varphi - 1 + \sqrt{\varphi^2 - 2\varphi}}, \quad (2)$$
$$c_1 = c_2 = \varphi w.$$

In PSO-agent, we use an original version of PSO with intermediate parameter φ. Figure 3 shows an evolution process of PSO-agent.

3.3. DE-Agent Model. Differential evolution (DE) is a metaheuristic method that optimizes a problem by iteratively trying to improve a candidate solution with regard to a given measure of quality. In the DE, at first, the initial solution vector group should be generated randomly. The generated solution vectors are updated by performing three processes which are replacement, making a trial vector, and crossover.

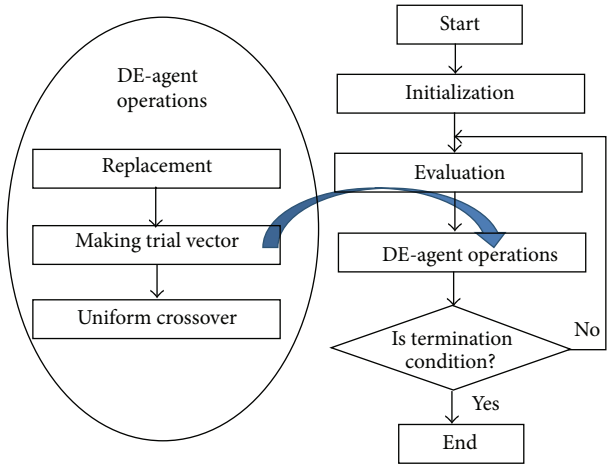


Figure 4: Evolution process of a DE-agent.

The replacement is a process that if a candidate solution made by crossover is better than a present solution, a present solution is updated by a candidate solution. The trial vector is a vector made by the following formulae to combine the existing vectors from the population [26]. Consider the following:

$$\overline{V}_{G+1} = \overline{X}_{r1,G} + F \cdot \left(\overline{X}_{r2,G} - \overline{X}_{r3,G}\right), \quad (3)$$

where $\overline{X}_{r1,G}$, $\overline{X}_{r2,G}$, and $\overline{X}_{r3,G}$ are randomly selected solutions in current population and F is a real positive coefficient.

In DE-agent, we use a standard version of DE with a uniform crossover. Figure 4 shows an evolution process of PSO-agent. A candidate vector $U_{i,G+1}$ is generated by uniform crossover operation with randomly selected solution $X_{i,G}$ in current population and the trial vector $V_{i,G+1}$ as follows:

$$U_{i,G+1} = \begin{cases} V_{i,G+1} & \text{for rand}() < \text{CR} \\ X_{i,G} & \text{for others,} \end{cases} \quad (4)$$

where the rand( ) means a random number between 0 and 1 and CR is probability of crossover.

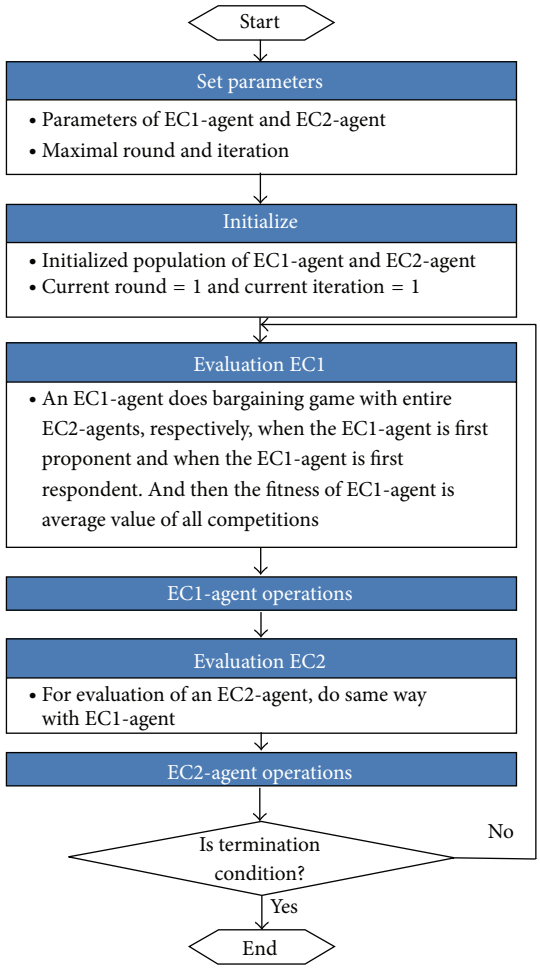


Figure 5: Coevolution model between two EC-agents in bargaining game.

4. Coevolution Model

The co-evolution model between two EC-agents in bargaining game is presented in Figure 5. After the solution groups of two kinds of EC-agents are randomly generated, each group is evaluated and evolved step by step. When one group of solutions is evaluated, entire solutions of another group are used for the counterparts in the bargaining game. And the player begin the bargaining game twice as a proponent or a respondent against each counterpart. Finally, the fitness value of solution is calculated by averaging all earns of total games. For example, when the number of entire solution is 30, two rounds of the bargaining game were conducted for each counterpart (beginning as a proponent, beginning as a respondent) to gain 60 different earns in total. The values were divided by 60 to determine the fitness of the solution.

5. Experimental Results

This section shows experimental results based on adaptive EC-agents. EC-agents have inter alia parameters which have effects on the performance. In a GA-agent, the parameters are a probability of crossover and mutation; in a PSO-agent, they are an intermediate parameter and maximum velocity; in a DE-agent, they are a coefficient F and probability of crossover. We examined the impact of variations of the above parameters on the experimental results.

In order to observe the coevolution among EC-agents in a bargaining game, three experiments on GA-agent versus PSO-agent, GA-agent versus DE-agent, and PSO-agent versus DE-agent were conducted.

5.1. Experimental Environment. In order to create an experimental environment, we set the simulation parameters as follows:

(i) population size: 30;

(ii) maximum iteration: 10,000;

(iii) maximum round in bargaining game: 5;

(iv) number of counterparts: 30 (entire population).

5.2. Experiment of Single EC-Agent. In this experiment, each EC-agent is tested on bargaining game with the fixed group of the counterpart's solutions in order to determine the optimal control parameter of each EC-agent.

5.2.1. GA-Agent. The control parameters of GA-agent are a crossover rate and mutation rate. As shown in Figure 6, the best performance of GA-agent in bargaining game was observed under the crossover rate of 0.9 and mutation rate of 0.05.

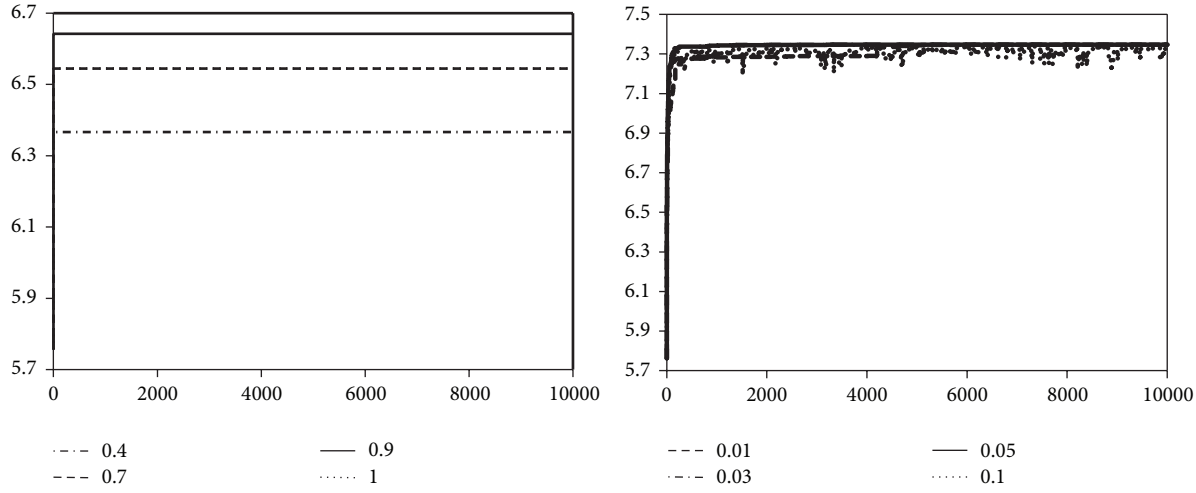
5.2.2. PSO-Agent. The control parameters of PSO-agent are an intermediate parameter φ and maximum velocity $v_{\max}$. As shown in Figure 7, the best performance of PSO-agent in bargaining game was observed under $\varphi = 0.9$ and $v_{\max}$ = search space/5. Here, search space (SS) is 10; thus, $v_{\max} = 2$.

5.2.3. DE-Agent. The control parameters of DE-agent are a coefficient F and crossover rate CF. As shown in Figure 8, there is very little difference in the performance of DE-agent in bargaining game with regard to two control parameters. Thus, we adopt that $F = 0.7$ and CF = 0.5 which are generally used.

5.3. Experiment of Coevolution between Two EC-Agents

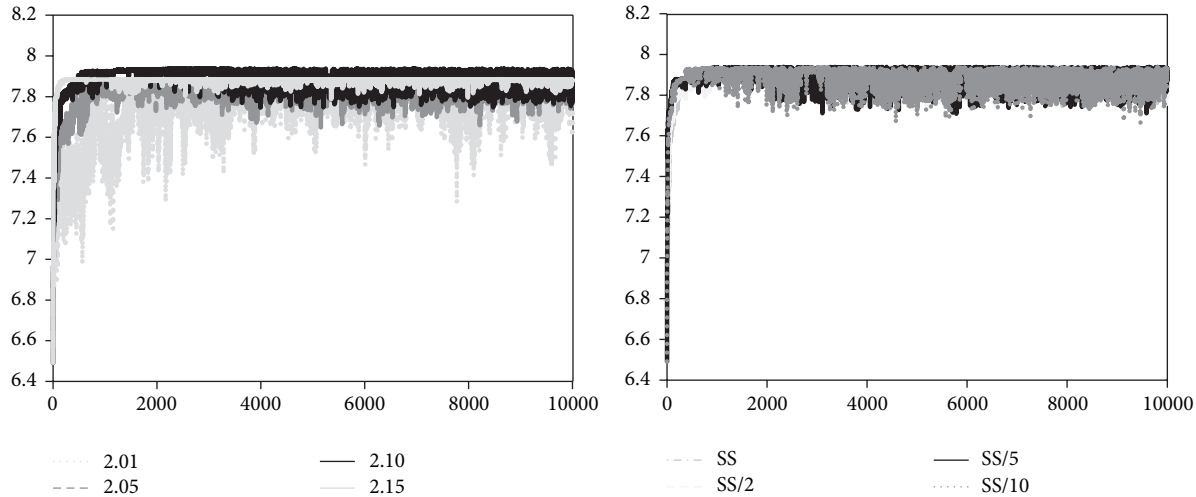
5.3.1. GA-Agent versus PSO-Agent. The result of the bargaining game by means of coevolution between the GA-agent and PSO-agent is shown in Figure 9. The GA-agent was set to the optimal environment determined in Section 5.2.1 and the PSO-agent to that in Section 5.2.2. As you can see, the PSO-agent is superior to the GA-agent in the coevolution-based bargaining game.

5.3.2. GA-Agent versus DE-Agent. The result of the bargaining game by means of coevolution between the GA-agent and DE-agent is shown in Figure 10. The GA-agent was set to the optimal environment determined in Section 5.2.1 and the



(a) Crossover rate (mutation rate = 0) (b) Mutation rate (crossover rate = 0.9)

Figure 6: GA-agent tests.



(a) φ ($v_{\max}$ = SS/2) (b) $v_{\max}$ (φ = 2.10)

Figure 7: PSO-agent tests.

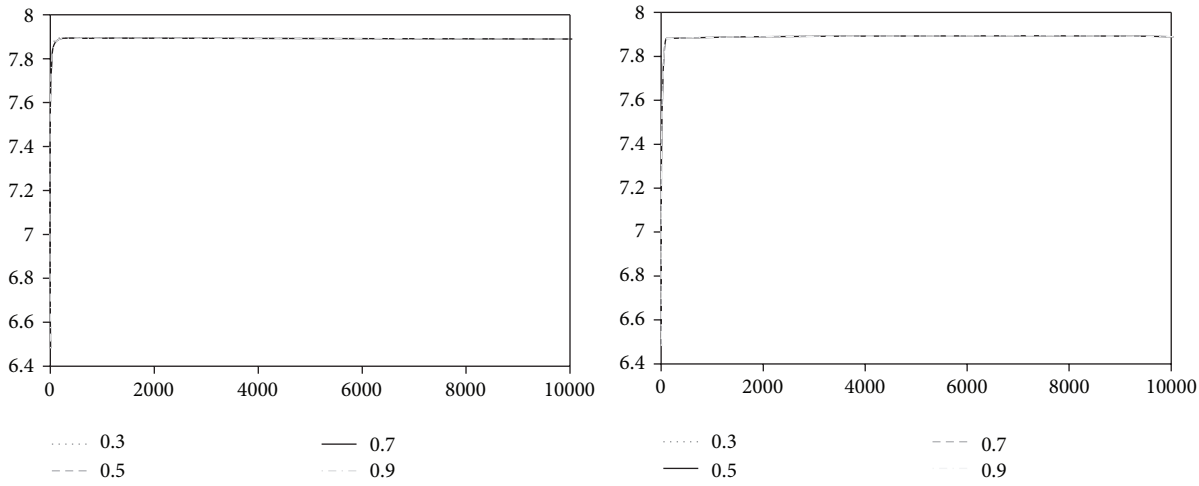
DE-agent to that in Section 5.2.3. As you can see, the GA-agent is superior to the DE-agent in the coevolution-based bargaining game.

5.3.3. PSO-Agent versus DE-Agent. The result of the bargaining game by means of coevolution between the PSO-agent and DE-agent is shown in Figure 11. The PSO-agent was set to the optimal environment determined in Section 5.2.2 and the DE-agent to that in Section 5.2.3. As you can see, the PSO-agent is superior to the DE-agent in the coevolution-based bargaining game.

5.4. Discussion. Firstly, performance measure among the EC-agents with respect to payoff is observed by changing the control parameters. The simulation results show the following implications. The control parameters of a GA-agent and PSO-agent have more influence on the performance than those of a DE: the probabilities of crossover and mutation of a GA-agent and the value of intermediate parameter and maximum velocity of a PSO-agent have effects on the performance but the probabilities of crossover and coefficient of a DE-agent have little effects on the performance.

Secondly, the coevolutionary process among three kinds of EC-agents which are GA-agent, PSO-agent, and DE-agent is tested to observe which EC-agent shows the best performance in the bargaining game. The simulation results show that a PSO-agent is better than a GA-agent and a DE-agent and that a GA-agent is better than a DE-agent with respect to coevolution in bargaining game.

In order to understand why a PSO-agent is the best among three kinds of EC-agents in the bargaining game,



(a) F (CF = 0.5) (b) CF (F = 0.7)

Figure 8: DE-agent tests.

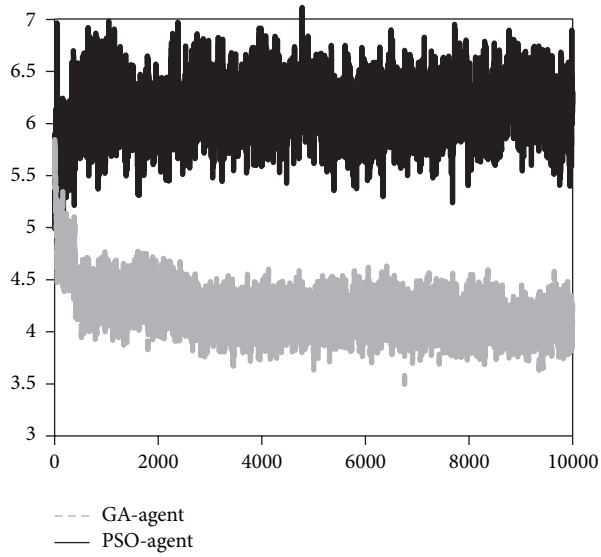


Figure 9: GA-agent versus PSO-agent.

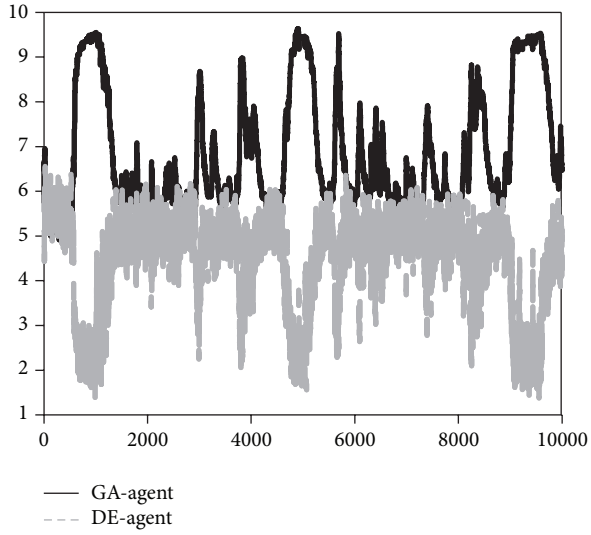


Figure 10: GA-agent versus DE-agent.

we observed the strategies of EC-agents after completion of game. Figure 12 shows the strategies of a GA-agent and a PSO-agent after completion of game. When the PSO-agent is a proponent, he suggests a small quantity of properties to the opponent, but when he is a respondent, he desired a large quantity. In contrast, when the GA-agent is a proponent, he suggests a large quantity to the opponent, but when he is a respondent, he desired a small quantity. In case of bargaining game between a PSO-agent and a DE-agent, the strategy of a DE-agent is similar to GA-agent of the figure. This indicated that the PSO-agent evolves in direction of the strategy to gain as much as possible at the risk of gaining no property upon failure of the transaction, while the GA-agent and the DE-agent evolve in direction of the strategy to accomplish the transaction regardless of the quantity.

6. Conclusion

The interaction and coevolutionary process among the heterogeneous EC-agents are studied to observe the performance of the bargaining game. This paper investigates the nature of interaction and coevolutionary process in order to understand the pattern of action of three kinds of EC-agents and also identifies the principal parameters that influence the performance of agents. The simulation results show that the control parameters of a GA-agent and PSO-agent have more influence on the performance than those of a DE. Furthermore, the simulation results also show that a PSO-agent is better than a GA-agent and a DE-agent with respect

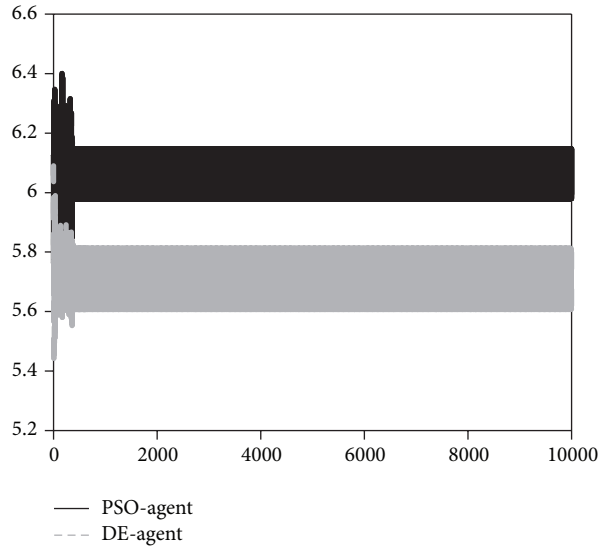


Figure 11: PSO-agent versus DE-agent.

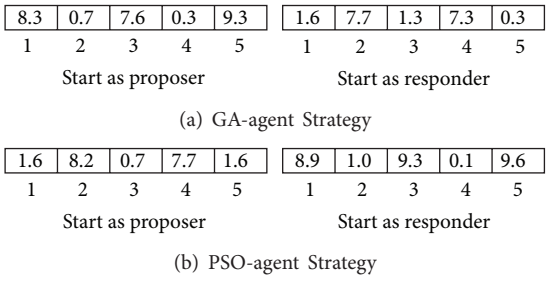


Figure 12: Comparison of strategies after completion of game.

to coevolution in bargaining game. We expect the analysis on the characteristics of artificial agents to help the researchers who study the game theory using artificial agents.

Conflict of Interests

The author declares that there is no conflict of interests regarding the publication of this paper.

References

[1] I. Ståhl, *Bargaining Theory*, Stockholm School of Economics, Stockholm, Sweden, 1971.

[2] A. Rubinstein, "Perfect equilibrium in a bargaining model," *Econometrica*, vol. 50, no. 1, pp. 97–109, 1982.

[3] T. Omoto, K. Kobayashi, and M. Onishi, "Bargaining model of construction dispute resolution," in *Proceedings of the IEEE International Conference on Systems, Man and Cybernetics*, vol. 7, pp. 7–12, October 2002.

[4] S. Berninghaus, W. Güth, R. Lechler, and H.-J. Ramser, "Decentralized versus collective bargaining—an experimental study," *International Journal of Game Theory*, vol. 30, no. 3, pp. 437–448, 2002.

[5] M. Nakayama, "E-commerce and firm bargaining power shift in grocery marketing channels: a case of wholesalers' structured document exchanges," *Journal of Information Technology*, vol. 15, no. 3, pp. 195–210, 2000.

[6] S. Matwin, T. Szapiro, and K. Haigh, "Genetic algorithms approach to a negotiation support system," *IEEE Transactions on Systems, Man and Cybernetics*, vol. 21, no. 1, pp. 102–114, 1991.

[7] K. M. Page, M. A. Nowak, and K. Sigmund, "The spatial ultimatum game," *Proceedings of the Royal Society B: Biological Sciences*, vol. 267, no. 1458, pp. 2177–2182, 2000.

[8] D. D. B. van Bragt and J. A. La Poutrè, "Co-evolving automata negotiate with a variety of opponents," in *Proceedings of the Congress on Evolutionary Computation (CEC '02)*, vol. 2, pp. 1426–1431, Honolulu, Hawaii, USA, May 2002.

[9] K. Takadama, Y. L. Suematsu, N. Sugimoto, N. E. Nawa, and K. Shimohara, "Towards verification and validation in multiagent-based systems and simulations: analyzing different learning bargaining agents," in *Proceedings of the 4th Workshop on Multi-Agent Based Simulation*, pp. 18–32, 2003.

[10] F. Zhong, S. O. Kimbrough, and D. J. Wu, "Cooperative agent systems: artificial agents play the ultimatum game," in *Proceedings of the 35th Annual Hawaii International Conference on System Sciences*, pp. 2169–2177, 2002.

[11] D. J. Cooper, N. Feltovich, A. E. Roth, and R. Zwick, "Relative versus absolute speed of adjustment in strategic environments: responder behavior in ultimatum games," *Experimental Economics*, vol. 6, no. 2, pp. 181–207, 2003.

[12] B. Grosskopf, "Reinforcement and directional learning in the ultimatum game with responder competition: experimental economics," *Experimental Economics*, vol. 6, no. 2, pp. 141–158, 2003.

[13] A. E. Roth and I. Erev, "Learning in extensive-form games: experimental data and simple dynamic models in the intermediate term," *Games and Economic Behavior*, vol. 8, no. 1, pp. 164–212, 1995.

[14] J. H. Kagel, C. Kim, and D. Moser, "Fairness in ultimatum games with asymmetric information and asymmetric payoffs," *Games and Economic Behavior*, vol. 13, no. 1, pp. 100–110, 1996.

[15] S. J. Burnell, L. Evans, and S. Yao, "The ultimatum game: optimal strategies without fairness," *Games and Economic Behavior*, vol. 26, no. 2, pp. 221–252, 1999.

[16] T. D. Stanley and U. Tran, "Economics students need not be greedy: fairness and the ultimatum game," *Journal of Socio-Economics*, vol. 27, no. 6, pp. 657–664, 1998.

[17] R. H. Thaler, "Anomalies: the ultimatum game," *Journal of Economic Perspectives*, vol. 2, pp. 195–206, 1988.

[18] R. Suleiman, "Expectations and fairness in a modified Ultimatum game," *Journal of Economic Psychology*, vol. 17, no. 5, pp. 531–554, 1996.

[19] S.-C. Chang, J.-I. Yun, J.-S. Lee, S.-U. Lee, N.-P. Mahalik, and B.-H. Ahn, "Analysis on the parameters of the evolving artificial agents in sequential bargaining game," *IEICE Transactions on Information and Systems*, vol. 88, no. 9, pp. 2098–2101, 2005.

[20] M. H. Seong and S. Y. Lee, "A bargaining game design using co-evolution analysis between artificial agents," *Advanced Science and Technology Letters*, vol. 46, pp. 10–14, 2014.

[21] M.-H. Seong and S.-Y. Lee, "A bargaining game using artificial agents based on genetic algorithms and particle swarm optimization," *International Journal of Software Engineering and Its Applications*, vol. 8, no. 5, pp. 205–218, 2014.

[22] J. H. Holland, *Adaptation in Natural and Artificial System*, University of Michigan Press, Ann Arbor, Mich, USA, 1975.

[23] D. E. Goldberg and K. H. KlÄosener, "A comparative analysis of selection schemes used in genetic algorithms," in *Foundation of Genetic Algorithms*, G. Rawlins, Ed., pp. 69–93, Morgan Kaufmann, San Mateo, Calif, USA, 1991.

[24] R. C. Eberhart and J. Kennedy, "A new optimizer using particle swarm theory," in *Proceedings of the 6th International Symposium on Micro Machine and Human Science (MHS '95)*, pp. 39–43, IEEE Service Center, Nagoya, Japan, October 1995.

[25] M. Clerc and J. Kennedy, "The particle swarm-explosion, stability, and convergence in a multidimensional complex space," *IEEE Transactions on Evolutionary Computation*, vol. 6, no. 1, pp. 58–73, 2002.

[26] R. Storn and K. Price, "Differential evolution—a simple and efficient heuristic for global optimization over continuous spaces," *Journal of Global Optimization*, vol. 11, no. 4, pp. 341–359, 1997.

Hindawi Publishing Corporation
Advances in Multimedia
Volume 2015, Article ID 380849, 7 pages
http://dx.doi.org/10.1155/2015/380849

Research Article

Preprocessing Techniques for High-Efficiency Data Compression in Wireless Multimedia Sensor Networks

Junho Park[1] and Jaesoo Yoo[2]

[1]*Agency for Defense Development, Daejeon 305-600, Republic of Korea*
[2]*School of Information and Communication Engineering, Chungbuk National University, Cheongju, Chungbuk 361-763, Republic of Korea*

Correspondence should be addressed to Jaesoo Yoo; yjs@chungbuk.ac.kr

Received 29 August 2014; Accepted 3 November 2014

Academic Editor: Seungmin Rho

Copyright © 2015 J. Park and J. Yoo. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

We have proposed preprocessing techniques for high-efficiency data compression in wireless multimedia sensor networks. To do this, we analyzed the characteristics of multimedia data under the environment of wireless multimedia sensor networks. The proposed preprocessing techniques consider the characteristics of sensed multimedia data to perform the first stage preprocessing by deleting the low priority bits that do not affect the image quality. The second stage preprocessing is also performed for the undeleted high priority bits. By performing these two-stage preprocessing techniques, it is possible to reduce the multimedia data size in large. To show the superiority of our techniques, we simulated the existing multimedia data compression scheme with/without our preprocessing techniques. Our experimental results show that our proposed techniques increase compression ratio while reducing compression operations compared to the existing compression scheme without preprocessing techniques.

1. Introduction

In recent, with the development of hardware technologies and monitoring schemes, the applications for gathering multimedia data such as sound and image using multimedia sensors have been increased [1, 2]. As the multimedia data are very large over simple data in traditional sensor networks, the network lifetime of the sensor network is significantly reduced due to excessive energy consumption in particular nodes for transmitting the multimedia data [3]. In addition, the multimedia data increase the data transmission time and decline the data reception ratio. Consequently, the existing schemes based on the traditional sensor networks are not suitable for the environments to collect the multimedia data [3, 4].

It is necessary to use compression schemes to alleviate such problems. However, most of the existing compression schemes for sensor data are based on signal compression such as wavelet and variable quantization and code compression [5]. These studies are not suitable for the environments based on wireless sensor networks. The compression schemes for wireless multimedia sensor networks are at an early stage. Considering this, a novel compression scheme based on the Chinese remainder theorem for the multimedia data has been proposed in [6]. The compression scheme based on the Chinese remainder theorem considered the characteristics and limitation of wireless multimedia sensor networks. However, the existing compression scheme still suffers from energy consumption in the wireless multimedia sensor network with the limited energy.

In this paper, we propose preprocessing techniques for high-efficiency data compression in wireless multimedia sensor networks. The proposed techniques consider the characteristics of sensed multimedia data to perform the first stage preprocessing by deleting the low priority bits that do not affect the image quality. The second stage preprocessing is also performed for the undeleted high priority bits. By performing these two-stage preprocessing techniques, it is possible to reduce the multimedia data size in large.

The remainder of this paper is organized as follows. Section 2 overviews and analyzes the existing compression schemes. In Section 3, we present our preprocessing

techniques for high-efficiency data compression in wireless multimedia sensor networks. Section 4 shows the simulated experiments and compares the existing scheme with the proposed scheme. Finally, we present concluding remarks in Section 5.

2. Related Works

The existing compression schemes for multimedia data can be categorized under 1st and 2nd generation schemes [7]. The 1st generation schemes such as DCT based compression [8], EZW [9], SPIHT [10], and EBCOT [11] emphasize more on how well the information contained in a transformed multimedia data is efficiently encoded whereas the 2nd generation schemes such as Pyramidal [12], Directional Decomposition [13], Segmentation [14], and Vector Quantization [15] place more importance on how we can exploit and extract useful information from the multimedia data. However, the existing compression schemes require the high-computational power and large memory to process the compression. Because of the constrained hardware of a wireless sensor node, these studies are not suitable for the environments based on wireless sensor networks. Considering this, a compression scheme based on the Chinese remainder theorem for the multimedia data was proposed [6]. However, the existing compression scheme suffers from energy consumption in the wireless multimedia sensor network with the limited energy. Therefore, it is necessary to study a preprocessing technique considering the characteristics of the wireless multimedia sensor networks to improve the efficiency of compression scheme.

3. The Preprocessing Techniques for High-Efficiency Data Compression

In this paper, for the maximization of compression efficiency, we propose the preprocessing techniques that consist of dynamic area extraction and bit plane deletion before conducting compression scheme. By doing so, the proposed scheme reduces data compression operation, improves compression ratio, and minimizes energy consumption generated from data transmission by transmitting the remaining data instead of original multimedia sensor data.

3.1. Preprocessing Technique (1): Extracting the Dynamic Area. In general, the wireless multimedia sensor networks require the installation costs and distribute the few multimedia sensor nodes and many general sensor nodes together. As shown in Figure 1, the first detection is done through general scalar sensor nodes. When an abnormal signal (event) is detected, the near multimedia sensor nodes perform the second detection for the detailed monitoring. The position of a sensor node distributed to the network is fixed. As the multimedia sensor node is designed for the unidirectional shooting, it continuously shoots the image data of the space so that the abnormal signal is detected by adjusting the shooting angle and transmits the sensed data to the base station.

Figure 2 shows the characteristics of sensed images in the wireless multimedia sensor networks. As shown in the Figure 2, the wireless multimedia sensor node continuously shoots the image of space that the abnormal signal is detected so that a dynamic area and a static area with a considerable size occur according to the time. By considering the characteristics, the transmission of the whole sensed data causes the unnecessary communication cost. It also reduces network lifetime. In order to solve such problems, the proposed scheme extracts and compresses the high efficient dynamic area.

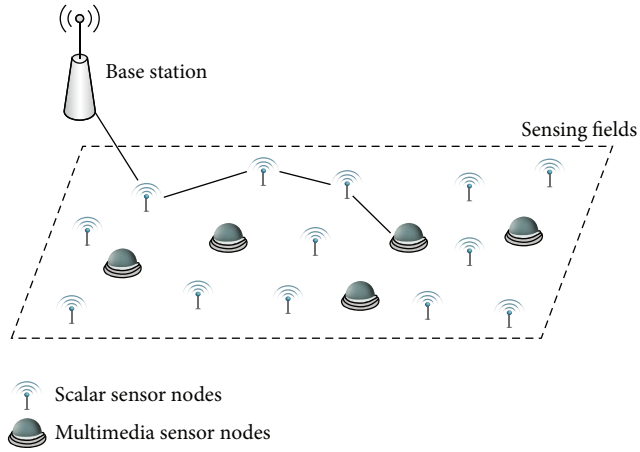


Figure 1: Deployment of wireless multimedia sensor networks.

First of all, it is important to detect the dynamic area in the sensed data. As it needs a high arithmetic operation cost to compare all pixels in the detection stage of the dynamic area, it is not efficient. Therefore, the proposed scheme generates the virtual comparison block through the pixel clustering and the detection of the image change and uses it as the transmission unit as shown in Figure 3. As the virtual comparison block is utilized as a transmission unit, there should be no effect on the compression based on the Chinese remainder theorem [3]. The conditions of the virtual comparison block are as follows by the definition of compression scheme based on the Chinese remainder theorem.

Condition 1. As the continuous decimal numbers to utilize the Chinese remainder theorem are at least two or more, it must be possible to express the comparison block data with two continuous decimal numbers.

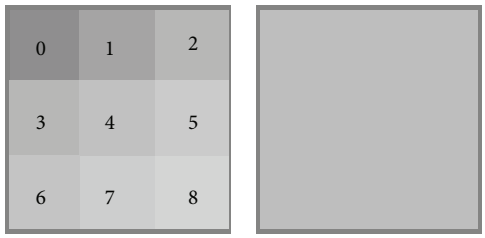
Condition 2. As the actual transmission data to the base station is the remainder, the remainder is below the maximum expression range of a specific variable type for the maximum efficiency.

Condition 3. For the easy restoration of original data and block data, it is a structure of square which is applicable for the QCIF format.

By the conditions above, the maximum block size for possible utilization is 3×3 pixels (the proof is omitted due to the space limit).

(a) t_0 (b) t_1

FIGURE 2: Characteristic of sensed images in the wireless multimedia sensor networks.



(a) Virtual comparison block #n (b) Average value of virtual comparison block #n

FIGURE 3: Virtual comparison block and clustering operation.

The virtual comparison block with a grid shape is generated to the sensed image. As in (1), the proposed scheme clusters the colors of all pixels inside the corresponding virtual comparison block and computes their average values. At this time, if the average values of the colors in the virtual comparison blocks of the initially sensed images and the currently sensed images are above the threshold value, they should be recognized as the dynamic areas as follows:

$$\left|\text{firstImgBlock \#n.avrValue} - \text{curImgBlock \#n.avrValue}\right| > \alpha. \quad (1)$$

Figure 4 shows the detection of the dynamic area and the extraction of the transmission area. Through the comparison of average values of colors in the virtual comparison block, the dynamic area that must be transmitted is recognized. The corresponding dynamic area is compressed based on the Chinese remainder theorem to transmit it to the base station. At this time, when the packets are transmitted in the virtual comparison block unit, unnecessary data transmission occurs due to header and trailer. To solve such a problem, the proposed scheme transmits the dynamic area in a single packet through the establishment and extraction of the maximum transmission area. Through this process, the proposed scheme minimizes the energy consumption by the partial compression and transmission of the dynamic area.

3.2. Preprocessing Technique (2): Deleting Bit Plane Data. The sensor node is driven based on the limited energy and computing performance so that it needs an additional compression module to perform the data compression. However, it requires a lot of installation costs. Considering this, transmitting the original data was common in the existing scheme. Figure 5 shows the structure of multimedia sensor data in wireless multimedia sensor networks. The image data sensed from the wireless multimedia sensor network has a data bit structure of the pixel unit, and each pixel has eight bits (0~255) per color channel (R, G, B) as shown in Figure 5. The same bits are bound together to compose a bit plane. As a result, the color image is composed of 24 bit planes in total. While the data sizes of the bit plane are equivalent, the amount of their expressible information and the importance are different. For example, each bit of the most significant 7 bit plane can express 128, but each bit of the lowest significant 0 bit plane can express only 1. In other words, the most significant bit plane shows a big color change and the lowest bit plane shows the small color change.

Based on this analysis, Figure 6 shows the changes in image quality according to the bit plane deletion. When the most significant bit plane is deleted, serious damages to the quality of the original data occur. However, when the low significant bit plane data is deleted, it does not largely affect the quality of the original data. From the result, when all bit plane data cannot be transmitted, the high quality image can be maintained by deleting data near the lowest bit plane. In the proposed scheme, the preprocessing (2) is performed for the image data based on this fact.

According to the result from the preprocessing (2), few bit plane data are selected as transmission data. As a result, the proposed scheme minimizes the energy consumption and increases the lifetime of a whole network by utilizing this kind of preprocessing techniques.

4. Performance Evaluation

We have developed a simulator based on JAVA to evaluate the existing multimedia data compression scheme [6] with/without our preprocessing techniques. This simulation was carried out by constructing the performance evaluation environment shown in Table 1.

In order to carry out performance evaluation, we utilized the uncompressed MPEG-4 standard image provided by Xiph.org [16]. Figure 7 shows the sample images of uncompressed MPEG-4 standard images. This simulation was done

(a) t_0 (b) t_1

Figure 4: Detection of the dynamic area and extraction of the transmission area.

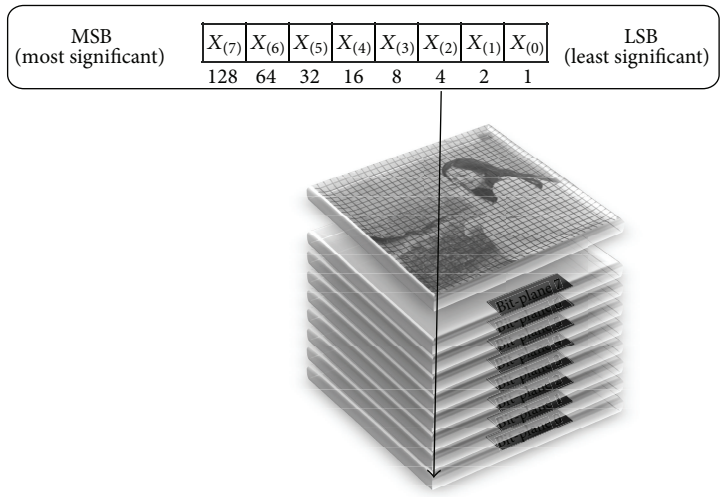


Figure 5: Structure of multimedia sensor data in wireless multimedia sensor networks.

Table 1: Simulation parameters.

Parameters	Values
Multimedia data	Uncompressed MPEG-4 standard images provided by Xiph.org and CCTV image
Length of multimedia data (frames)	50
Format of multimedia data (px × px)	CIF (352 × 288) QCIF (176 × 144)

Table 2: Characteristics of uncompressed MPEG-4 standard images [16].

	Resolution (px × px)	Size of images (Mbytes)	Frames	Class
(a) Akiyo	CIF (352 × 288)	CIF (44)	300	A
	QCIF (176 × 144)	QCIF (11)		
(b) News	CIF (352 × 288)	CIF (44)	300	B
	QCIF (176 × 144)	QCIF (11)		

targeting the image having CIF (full CIF) and QCIF (quarter CIF) resolution which are generally gathered by wireless multimedia sensor networks. In Table 2, the image classification indicates spatial complexity and motion amount, in which "A" is the image expressing a tiny level of spatial complexity and movement while "B" signifies the image expressing a mid-level of spatial complexity and movement [17]. In addition, the wireless multimedia sensor networks have a distribution characteristic and monitoring characteristic similar to that of closed circuit TV (CCTV). Therefore, in this simulation, the performance evaluation was conducted by collecting images of actual CCTV. The relevant images are CCTV images [18] of the fire occurrence at Busan Metro Daeti Station in Korea on August 27, 2012, and for simulation we converted the format to CIF and QCIF. Figure 8 shows the sample images of CCTV images.

Figure 9 shows the compression ratio per frame to standard image and CCTV image of the proposed scheme with preprocessing techniques. Performance evaluation was carried out by grafting preprocessing technique (1) and preprocessing technique (2) onto the existing scheme. Preprocessing technique (1) indicates dynamic area extraction and preprocessing technique (2) #2, #4, and #6 indicate

(a) Deletion of the most significant bit plane data (b) Deletion of the least significant bit plane data

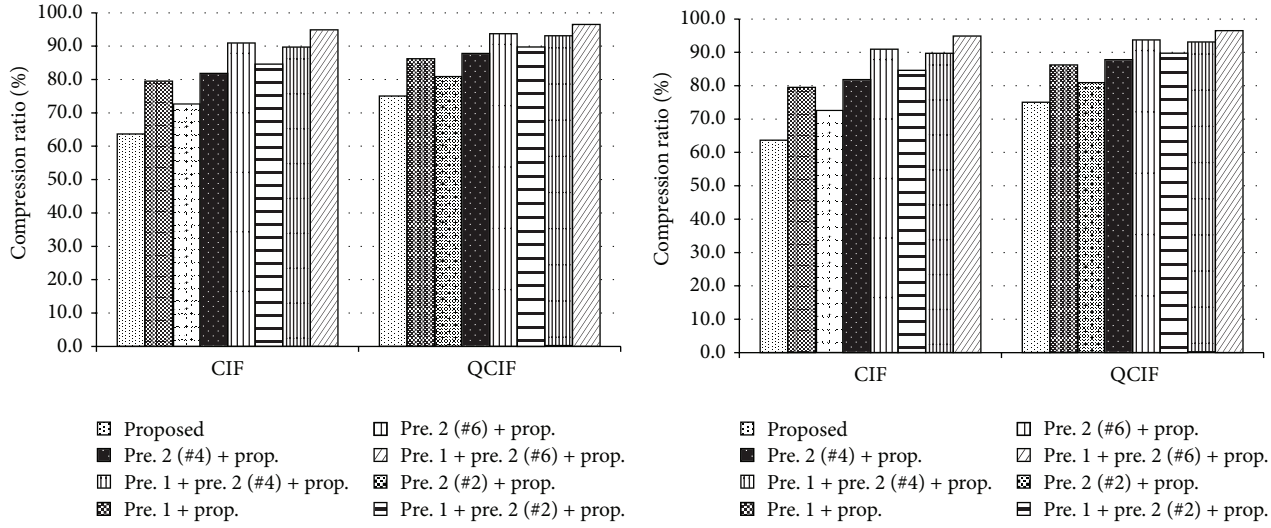
Figure 6: Changes in image quality according to the bit plane deletion.

(a) Akiyo (b) News

Figure 7: Sample images of uncompressed MPEG-4 standard images.

Figure 8: Sample images of CCTV image.

the number deleting the bit plane, respectively. According to the experimental result, in case preprocessing technique (1) is applied, the compression ratio improves as the area for compression is reduced by extracting dynamic area while transmitting the relevant area by compressing the area only. In addition, in case preprocessing technique (2) is applied, the compression ratio also improves since the number of bit planes for compression is reduced by adjusting the quality of multimedia sensor data through the deletion of bit planes according to applications. In case 1 bit plane is deleted, preprocessing technique (2) improves compression efficiency by 12.5% on the basis of grayscale image but, as much,



(a) Sample images

(b) CCTV image

Figure 9: Compression ratio per frame with preprocessing techniques.

image information is lost; therefore, proper setup should be done according to application. In addition, in the event of grafting preprocessing technique (1) onto CCTV image, image change severely comes up, which causes dynamic area to be wide extracted relatively, and consequently it does not serve to improve compression efficiency to a larger extent than optimized image. Nonetheless, preprocessing technique (2) belongs to arithmetic operation deleting bit plane, causing no big impact. As a result, the existing scheme with preprocessing technique (1) and the existing scheme with preprocessing technique (2) improve the data compression ratio by about 25% and 42.9%, respectively, over the existing scheme without preprocessing techniques. In addition, when preprocessing technique (1) and preprocessing technique (2) were simultaneously grafted, the existing scheme improves the data compression ratio by about 49.2% over the existing scheme without preprocessing techniques.

Figure 10 shows the compression arithmetic operation quantity in the existing scheme with preprocessing techniques. Preprocessing technique (1) requires per-pixel comparison operation with the previous image in order to extract the dynamic area, making it inevitable to carry out large-scale arithmetic operation. In order to reduce this, per-block data comparison is performed, but it also requires large-scale arithmetic operations. In the event of grafting preprocessing technique (2), the compression operation quantity is decreased, which can be explained by the fact that compression operations decrease as much because the bit plane deleted by virtue of simple deletion operation does not require compression operations. Preprocessing technique (2) gets improved in compression efficiency by 12.5% on the basis of grayscale image when 1 bit plane is deleted. However, since the loss of image information can occur, it is important to properly set up according to applications.

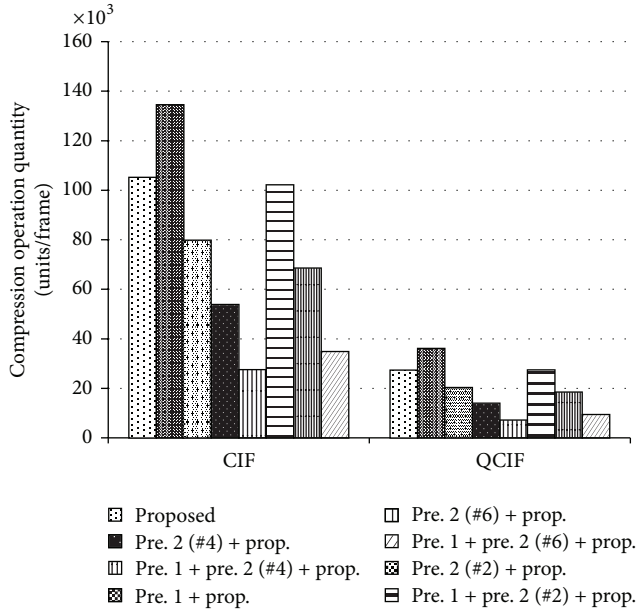


Figure 10: Compression operation quantity with preprocessing techniques.

5. Conclusion

In this paper, we have proposed preprocessing techniques for high-efficiency data compression in wireless multimedia sensor networks. To do this, we analyzed the characteristics of multimedia data under the environment of wireless multimedia sensor networks. The proposed scheme considers the characteristics of sensed multimedia data to perform the first compression by deleting the low priority bits that do not affect the image quality. The second stage compression is also

performed based on the Chinese remainder theorem for the undeleted high priority bits. By performing this two-stage compression, it is possible to reduce the multimedia data size in large. To show the superiority of our techniques, we simulated the existing multimedia data compression scheme with/without our preprocessing techniques. As a result, it was shown through performance evaluation that the proposed preprocessing scheme significantly increased compression ratio while reducing compression operation comparing to the existing compression schemes without preprocessing techniques. In the future work, we plan to study the effective transmission scheme considering the characteristics of compression data.

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

Acknowledgments

This research was supported by the MSIP (Ministry of Science, ICT and Future Planning), Korea, under the ITRC (Information Technology Research Center) Support Program (NIPA-2014-H0301-14-1022) supervised by the NIPA (National IT Industry Promotion Agency) and the C-ITRC (Convergence Information Technology Research Center) Support Program (NIPA-2014-H0401-14-1007) supervised by the NIPA (National IT Industry Promotion Agency), by the ICT R & D Program of MSIP/IITP [14-824-09-001], Development of High Performance Visual Big Data Discovery Platform for Large-Scale Real Time Data Analysis, and by the Ministry of Education (MOE) and National Research Foundation of Korea (NRF) through the Human Resource Training Project for Regional Innovation (no. 2013H1B8A2032298).

References

[1] S. M. Aziz and D. M. Pham, "Energy efficient image transmission in wireless multimedia sensor networks," *IEEE Communications Letters*, vol. 17, no. 6, pp. 1084–1087, 2013.

[2] P. Wang, R. Dai, and I. F. Akyildiz, "A differential coding-based scheduling framework for wireless multimedia sensor networks," *IEEE Transactions on Multimedia*, vol. 15, no. 3, pp. 684–697, 2013.

[3] 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.

[4] T. Ma, M. Hempel, D. Peng, and H. Sharif, "A survey of energy-efficient compression and communication techniques for multimedia in resource constrained systems," *IEEE Communications Surveys and Tutorials*, vol. 15, no. 3, pp. 963–972, 2013.

[5] W. C. Li, L. M. Ang, and P. S. Kah, "Survey of image compression algorithms in wireless sensor networks," in *Proceedings of the International Symposium on Information Technology (ITSim '08)*, pp. 1–9, August 2008.

[6] H. Lee, J. Park, D. Seong, and J. Yoo, "An energy-efficient data compression and transmission scheme in wireless multimedia sensor networks," *Journal of KIISE: Information Networking*, vol. 39, no. 3, pp. 258–266, 2012.

[7] L. W. Chew, L.-M. Ang, and K. P. Seng, "Survey of image compression algorithms in wireless sensor networks," in *Proceedings of the International Symposium on Information Technology (ITSim '08)*, pp. 1–9, IEEE, Kuala Lumpur, Malaysia, August 2008.

[8] D. Cruz, T. Ebrahimi, J. Askelof, M. Larsson, and C. Christopoulos, "Coding of still picture," in *Applications of Digital Image Processing*, vol. 4115 of *Proceedings of SPIE*, 2000.

[9] J. M. Shapiro, "Embedded image coding using zerotrees of wavelet coefficients," *IEEE Transactions on Signal Processing*, vol. 41, no. 12, pp. 3445–3462, 1993.

[10] A. Said and W. A. Pearlman, "A new, fast, and efficient image codec based on set partitioning in hierarchical trees," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 6, no. 3, pp. 243–250, 1996.

[11] D. Taubman, "High performance scalable image compression with EBCOT," *IEEE Transactions on Image Processing*, vol. 9, no. 7, pp. 1158–1170, 2000.

[12] P. J. Burt and E. H. Adelson, "The Laplacian pyramid as a compact image code," in *Proceedings of the Korean Institute of Information Scientists and Engineers*, vol. 31, pp. 532–540, 1983.

[13] A. Ikonomopoulos and M. Kunt, "High compression image coding via directional filtering," *Signal Processing*, vol. 8, no. 2, pp. 179–203, 1985.

[14] L. Ghouti, A. Bouridane, and M. K. Ibrahim, "Image compression using texture modeling," in *Proceedings of the IEEE International Symposium on Circuits and Systems (ISCAS '05)*, vol. 3, pp. 2313–2316, May 2005.

[15] G. F. McLean, "Vector quantization for texture classification," *IEEE Transactions on Systems, Man and Cybernetics*, vol. 23, no. 3, pp. 637–649, 1993.

[16] Xiph.Org Foundation, 2013, http://www.xiph.org/.

[17] Xiph.org Video Test Media, 2013, http://media.xiph.org/video/derf/.

[18] *Fire Occurrence at Busan Metro Daeti Station in Korea on August 27, 2012*, 2012, http://www.youtube.com/watch?v=Q-4KbAFEiEI.

Hindawi Publishing Corporation
Advances in Multimedia
Volume 2015, Article ID 956416, 5 pages
http://dx.doi.org/10.1155/2015/956416

Research Article

Security Requirements for Multimedia Archives

Sang Bae Park

KISTI, 245 Daehak-ro, Yuseong-gu, Daejeon 305-06, Republic of Korea

Correspondence should be addressed to Sang Bae Park; plucky@kisti.re.kr

Received 29 August 2014; Accepted 21 November 2014

Academic Editor: Seungmin Rho

Copyright © 2015 Sang Bae Park. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

With the explosive growth of various multimedia contents, digital archives are used to store those contents accordingly. In contrast to the traditional storage systems in which data lifetime is measured in months or years, data lifetime in the archive is measured in decades. This longevity of contents causes new security issues that threat the archive systems. In this paper, we discuss these new security issues in perspective. And we suggest some security requirements for digital archives.

1. Introduction

Now digital archives are increasingly being used to store digital contents that need to be preserved for a long time. Various kinds of multimedia contents, for example, cultural contents, academic journal, news, and so forth, are increasing very rapidly. Moreover, many existing contents are transferred into a digital multimedia format for availability and long-term preservation. Some digital contents should be preserved for a period of time. For example, the medical center has to store the patient's treatment for 10 years in republic of Korea. By the copyright law, copyright is effective for 70 years after the author's death. These kinds of contents should be carefully managed.

In order for the contents in such archives to be useful, there are some properties such as availability, integrity, and authenticity that should be protected. Generally, current storage systems adopt many security mechanisms, including access control, authentication, and encryption [1–3]. In contrast to traditional storage systems in which contents lifetimes are measured in months or possibly years, contents lifetimes in archive systems are measured in decades. For this longevity of contents, the security mechanisms for traditional storage system have some limitations. Primitives including block ciphers and hash functions do not guarantee robustness in the long term, it is a big challenge how to achieve long-term security [4–6].

In this paper, we discuss some security issues in digital archive systems and the plan for long-term preservations. Since a single cryptographic primitive cannot guarantee long-term security, we should consider additional physical protection methods and proper security policy. For example, write-once media can reduce the burden for authentication and integrity of stored contents. If we implement a hybrid-storage system with general storage and write-once media, we can store content in general storage and store log information in write-once media.

This paper is organized as follows. In Section 2, we briefly introduce a cryptographic background in information security. In Section 3, we discuss the long-term security issues, including the lifespan of cryptographic primitives, cryptographic keys, and other issues related to digital archive systems. In Section 4, we deal with required services for digital archives and update procedure for contents in archives.

2. Cryptographic Background

In this chapter, we briefly introduce some concepts and techniques for information security. For information security, we consider the following properties. Confidentiality guarantees that only authorized user can access the information. Authentication is for proving the originality. Integrity guarantees that there is no alteration. For satisfying these properties, we use physical protection, technical protection, and security policy. Cryptography is the technical approach for information security. Basic cryptographic primitives are symmetric key encryption, asymmetric key encryption, digital signature,

hash function, and PRNG (pseudo random number generator) [7].

Symmetric key encryption is for confidentiality. There are block ciphers and stream ciphers. Encryption makes plain text into cipher text with encryption key and decryption is its reverse process. Since encryption key and decryption key are the same, we call this function symmetric key encryption. For example, DES, AES, and RC4 are famous and are widely adopted [8, 9]. Symmetric key encryption is fast and efficient, but there is a problem how to share the key between message sender and receiver.

Asymmetric key encryption is also for confidentiality. Users make a pair of keys, public key and private key. The public key is used for encryption and the private key is for decryption. Since the public key is open to all users, key management for encryption is more convenient than symmetric key encryption. The most famous algorithm is RSA [10].

Hash function produces a fixed length random sequence for any input. This is for checking the integrity. MD4, MD5, and SHA-1 are famous hash functions [11–13]. Particularly, keyed hash function is called MAC (message authentication code).

A digital signature is an application of symmetric key encryption. Signer makes a hash value of the given message into a digital signature with the signer's private key. The verifier can check the authentication with the signer's public key. There are RSA and DSA [10, 14].

PRNG is used for making a random number. Unpredictability is most important for secure cryptographic protocols. Most cryptographic protocols including key management start from selecting random numbers.

Using these cryptographic primitives, people make cryptographic protocols for specific purposes. For confidence of the user's public key, we construct a TTP (trusted third party), the so-called CA (certificate authority). CA issues a digital signature for user's public key. People can check whether the user's public key is valid or not. This signature, including user's public key, is called a certificate. The PKI (public key infrastructure) includes CA and its service for secure application of asymmetric key cryptography.

Data enveloping is a practical approach for a content encryption. The sender makes a random session key and encrypts the session key with the receiver's public key. Then the sender encrypts main contents with the session key by symmetric key encryption. This approach has some advantages. At first, using symmetric key encryption for bulk data is efficient. Then the receiver can easily recover the whole message without a sharing process.

Another TTP service is a timestamp. This service is issuing a signature at that point of time. If the signer includes a timestamp in its signature, the verifier can check when the signature is generated.

For general storage service, there are some protocols. Since the size of stored data is growing more and more, transfer time became expensive. Proof of retrievability is for lessening this problem [15]. This protocol is that storage provider shows that user's data is really in the storage without transferring the whole data. Another protocol for storage service is a zero remnant protocol [16]. This protocol is verifying that there is no remnant after user's data deletion request.

3. Long-Term Security Issues

In this chapter, we discuss some security issues arising in digital archive systems. We consider the security of cryptographic primitives and related security protocols, lifetime of cryptographic keys, and other issues for long-term security.

3.1. Security of Cryptographic Primitives. Cryptographic primitives are basic tools for information security. Generally, we consider that cryptographic primitives are always secure. Though cryptographic primitives are secure now, these could be insecure in the future. There have been many researchers who try to find a new way to exploit cryptographic primitives' weakness.

In 1976, US government published the standard block cipher DES. DES had been used widely in many areas. At that time, 56-bit encryption key is sufficient. Because there was lack of computing power for 2^56 brute force, DES was considered secure. But, by the late 1990s, computers were so cheap and powerful that a 2^56 brute force search for the key became a feasible task. Moreover, dedicated cryptanalysis has been developed. Differential cryptanalysis and linear cryptanalysis are successful methods finding the key less than exhaustive search [17, 18].

Like block ciphers, hash functions are also mortal. The most famous hash functions MD-series, MD4, MD5, and MD5, are considered insecure, after Wang and Yu published collision for those hash functions that is a pair of different messages producing the same hash value [19].

The collisions of hash function cause a serious problem for digital signature using that hash function. Figure 1 shows how to make a fake message for a given digital signature. Collisions of hash functions nullify the authenticity of the digital signature. But there are still many private CAs adopting MD5 hash function. Certificates from those CA could be forged at a tolerable cost.

The security of cryptographic primitives determines the security of cryptographic protocols and services that consist of cryptographic primitives. For example, cipher suite of web security protocol SSL/TLS includes a cipher RC4 and hash functions MD4, MD5. The careless choosing of a cipher suite can cause the whole transaction insecure.

Table 1 shows a part of the known cryptanalysis for ciphers and hash functions.

Single cryptographic primitive might not guarantee long-term security. So we should continuously monitor the security of cryptographic primitives and we make a plan for algorithm change and contents update.

3.2. Lifetime of Cryptographic Keys. Cryptographic keys are most important in information security. There are two kinds of cryptographic keys. One is for a symmetric key cryptography, and the other is for an asymmetric key cryptography. Symmetric key cryptography includes symmetric

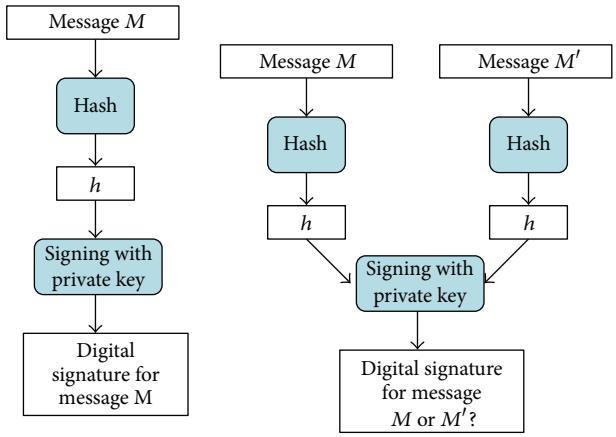


Figure 1: Digital signature process and collisions for hash function.

Table 1: Known attacks for cryptographic primitives.

Class	Algorithm	Known attack	Complexity
Block cipher	DES	Differential cryptanalysis	2^49
Block cipher	DES	Linear cryptanalysis	2^43
Stream cipher	RC4	Royal Holloway attack	2^24
Hash function	MD4	Differential cryptanalysis	2^8
Hash function	MD5	Differential cryptanalysis	2^19
Hash function	RIPEMD	Differential cryptanalysis	2^16

key encryption and MAC. Asymmetric key cryptography includes public key encryption and digital signature. Similar to cryptographic primitives, lifetime of cryptographic keys is shorter than preserved period. In this chapter, we discuss the lifetime of cryptographic keys and cryptographic outputs.

Symmetric keys are securely managed while the contents are preserved. For example, session keys for communications are used in just that session. But the encryption key for contents in storage should be managed for longer time. For long-term confidentiality, we should periodically update encrypted contents as the lifetime of cryptographic keys expires.

Asymmetric keys are usually included in X.509 certificate. There are two kinds of certificate even though the user adopts the same algorithm RSA for encryption and signature. Usually the valid period of the certificate is one year. For example, the valid period of certificates for internet banking is one year in republic of Korea. But the valid period of digital signature does not match that of the certificate. Since digital contents might be preserved in many decades, it is hard to guarantee the authenticity of the digital signature after decades. Moreover, we should manage private keys responding to certificates that have already expired because output contents live longer than certificates.

We also consider public security services dependent on cryptographic keys. Timestamp is a kind of digital signature applications. A single timestamp does not provide long-term security because it relies on a cryptographic hash function, a digital signature, or wide-visible media, which all are subject to security deterioration over time. We have to determine the lifespan of cryptographic key, signature, and archiving data very carefully. Table 2 shows the lifetime of cryptographic key and contents.

Table 2: Lifetime of cryptographic key and contents.

Class	Lifetime
Symmetric key	
Session key	Period of that session
Key for stored contents	Usually in years
Asymmetric key	
Certificate	1 or 3 years
Digital signature	Usually 5 years
Archives	Longer than decades

3.3. Other Issues for Long-Term Security. We need to consider other issues related to digital archiving systems such as the login system and the access control system. We examine not only the security of them but also how to delegate one's access right to others. Most login systems are based on cryptographic primitives. The password is stored in the system as encrypted form or its hash value. When underlying cryptographic primitives are broken, the administrator should change the whole login systems. Access control might be reinvestigated. Access right verification could be altered to be more sophisticated. For example, one rich man makes his will and stores it in the archive. After his demise, a bereaved family might access his will without revealing that to others.

We have to consider the content format too. There are continuously reports related to weakness of file format. We consider not only security but also backward compatibility for long-term availability. DRM (digital rights management) system is also very sensitive. Most DRM systems depend on system calls provided by the operating system. How long do we expect the backward compatibility of the operating system? We should consider a DRM system based on online cryptographic protocols.

Digital archives are designed for an outsourced storage service model which enables users to outsource the storage of their contents to remote storage service provider at a low cost. Since the management of storage is performed by a service provider, we should consider the balance between privacy and efficiency. For more privacy, we determine that the main actor for content protection is the user. But this may cause the security leakage by the individual's carelessness and inconsistency of the whole system security policy.

4. Requirements for Digital Archives

In this chapter, we discuss requirements for digital archive systems with issues in the previous chapter. For long-term confidentiality, there should be a process for updating encrypted data. The reencryption of large amounts of data must be done in a timely manner, especially if required for a key compromise or cryptographic primitives exploit. So we need robust high-speed encryption algorithm and reencryption procedure. For example, if a system chooses to

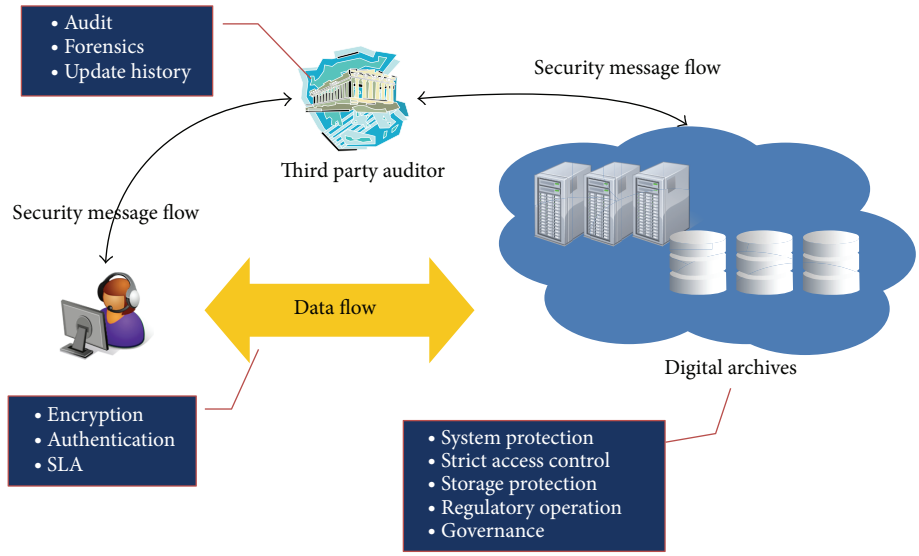


Figure 2: The third party auditor.

save time by encrypting over the old algorithm, it must have a way of dealing with key histories and key distribution. In contrast, if the system chooses to decrypt the data before applying the new algorithm, then it must have access to the user's key. In this case, the system should prevent a malicious user from the user's key and decrypted contents. For encryption update, we consider the following security requirements.

(i) Reencrypt encrypted data without revealing plain text to unauthorized users.

(ii) Make high-speed encryption for a large amount of data.

In Section 3, long-term authentication and integrity cannot be achieved by a single protection mechanism. Similar to confidentiality, we should consider a process for updating digital signatures. The digital signature update has to include some update history information. In that system, there are the following requirements.

(i) Make a signature update chain that cannot be reversed.

(ii) Secure delegation mechanism for signing keys.

We might consider the storage implementing with write-once media. This might be very expensive but easy for integrity. For more cost effective way, we can consider the following TTP service. We make another TTP called the third party auditor. Then digital archives stored sensitive log and audit in the third party auditor and the user verifies the log data with this TTP service. Figure 2 is a conceptual design of the third party audit.

For long-term security, we should carefully design an update procedure and period. There might be two kinds of update. One is a periodic update precautiously. The other is an emergency responding update for a key compromise or cryptographic primitives exploit. This emergency responding update is similar to disaster recovery. In this update procedure, the following should be included:

(i) policy for determining the update period;

(ii) monitoring plan;

(iii) update history management;

(iv) sealing process.

5. Conclusion

In this paper, we present some security issues related to digital archiving systems. Since digital archives preserve digital contents in very long term, we should consider the update of stored contents. These security issues should be considered before system design. And there should be the development cycle including design, implementation, monitoring and threat assessment, and periodic or emergency update. The focus of this paper was not to solve those problems which arise in long-term preservation but rather enumerate the requirements. We hope that by listing the security issues and requirements future efforts to build secure archives will be more focused. Moreover, we should consider that cryptographic approach cannot be a perfect solution without physical protection and well-established policy.

Conflict of Interests

The author declares that there is no conflict of interests regarding the publication of this paper.

References

[1] P. Anderson and L. Zhang, "Fast and secure laptop backups with encrypted de-duplication," *Proceedings of the 24th International Conference on Large Installation System Administration (LISA '10)*, 2010.

[2] G. Yamamoto, S. Oda, and K. Aoki, "Fast integrity for large data," *Proceedings of the Workshop on Software Performance Enhancement for Encryption and Decryption (SPEED '07)*, 2007.

[3] P. Maniatis, M. Roussopoulos, T. J. Giuli, D. S. H. Rosenthal, and M. Baker, "The LOCKSS peer-to-peer digital preservation system," *ACM Transactions on Computer Systems*, vol. 23, no. 1, pp. 2–50, 2005.

[4] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM Journal on Computing*, vol. 26, no. 5, pp. 1484–1509, 1997.

[5] J. Buchmann, A. May, and U. Vollmer, "Perspectives for cryptographic long-term security," *Communications of the ACM*, vol. 49, no. 9, pp. 50–55, 2006.

[6] J. Hughes and J. N. Roge, "Long-term security vulnerabilities of encrypted data," *Issues in Information Systems*, vol. 8, pp. 522–528, 2007.

[7] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, *Handbook of Applied Cryptography*, CRC Press Series on Discrete Mathematics and its Applications, CRC Press, Boca Raton, Fla, USA, 1996.

[8] National Bureau of Standard, *Data Encryption Standard (DES)*, FIPS Publication 46, 1977.

[9] NIST, "Advanced Encryption Standard (AES)," FIPS Publication 197, 2001.

[10] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, vol. 21, no. 2, pp. 120–126, 1978.

[11] R. Rivest and Network Working Group, "MD 4 message-digest algorithm," Tech. Rep. RFC 1320, 1992.

[12] Network Working Group and R. Rivest, "MD 5 Message-Digest Algorithm," RFC 1321, 1992.

[13] NIST, "Secure Hash Function," FIPS 180-1, 1995.

[14] NIST, "Digital Signature Standard (DSS)," FIPS 186, 1994.

[15] G. Ateniese, R. Burns, R. Curtmola et al., "Provable data possession at untrusted stores," in *Proceedings of the 14th ACM Conference on Computer and Communications Security (CCS '07)*, pp. 598–610, November 2007.

[16] A. Rahumed, H. C. H. Chen, Y. Tang, P. P. C. Lee, and J. C. S. Lui, "A secure cloud backup system with assured deletion and version control," in *Proceedings of the International Conference on Parallel Processing Workshops (ICPPW '11)*, pp. 160–167, September 2011.

[17] E. Biham and A. Shamir, "Differential cryptanalysis of DES-like cryptosystems," *Journal of Cryptology*, vol. 4, no. 1, pp. 3–72, 1991.

[18] M. Matsui, "Linear cryptanalysis method for DES cipher," in *Advances in Cryptology—EUROCRYPT '93*, vol. 765 of *Lecture Notes in Computer Science*, pp. 386–397, Springer, Berlin, Germany, 1994.

[19] X. Wang and H. Yu, "How to break MD5 and other hash functions," in *Advances in Cryptology—EUROCRYPT 2005*, vol. 3494 of *Lecture Notes in Computer Science*, pp. 19–35, Springer, Berlin, Germany, 2005.

Hindawi Publishing Corporation
Advances in Multimedia
Volume 2015, Article ID 420689, 7 pages
http://dx.doi.org/10.1155/2015/420689

Research Article

Discovering Congested Routes Using Vehicle Trajectories in Road Networks

Kyoung Soo Bok,[1] He Li,[2] Jong Tae Lim,[1] and Jae Soo Yoo[1]

[1] *School of Information and Communication Engineering, Chungbuk National University, 52 Naesudong-ro, Chungbuk, Seowon-Gu, Cheongju 362-763, Republic of Korea*
[2] *School of Software, Xidian University, No. 2 South Taibai Road, Xi'an City, Shaanxi 710071, China*

Correspondence should be addressed to Jae Soo Yoo; yjs@chungbuk.ac.kr

Received 28 August 2014; Accepted 23 October 2014

Academic Editor: Seungmin Rho

Copyright © 2015 Kyoung Soo Bok et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

The popular route recommendation and traffic monitoring over the road networks have become important in the location-based services. The schemes to find out the congested routes were proposed by considering the number of vehicles in a road segment. However, the existing schemes do not consider the features of each road segment such as width, length, and direction in a road network. Furthermore, the existing schemes fail to consider the average moving speed of vehicles. Therefore, they can detect the incorrect density routes. To overcome such problems, we propose a new discovering scheme of congested routes through the analysis of vehicle trajectories in a road network. The proposed scheme divides each road into segments with different width and length in a road network. And then, the congested road segment is detected through the saturation degree of the road segment and the average moving speed of vehicles in the road segment. Finally, we compute the final congested routes by using a clustering scheme. The experimental results have shown that the proposed scheme can efficiently discover the congested routes in the different directions of the roads.

1. Introduction

Recently, with the increase of the use of mobile devices, the location-based services are becoming increasingly popular. Since the rapidly increased satellites and GPS (global position system) technologies have developed, it is possible to collect a large amount of trajectory data of moving objects such as the vehicle position data, hurricane track data, and animal movement data [1–4]. The analysis over these trajectory data is becoming important for many applications, such as meteorological observation and forecast, animal habits observation, road traffic situation analysis, and navigation in transportations [5–9]. According to the recorded trajectory data and road networks, the moving pattern, traffic situation, and road recommendation services can be supported [1, 2, 10–12].

Recently, with the continuously increasing vehicles, the route recommendation service is becoming more and more important [1, 4, 7, 8, 13–15]. For road network based applications, the mobility of the vehicle is road network constrained. Most of the existing schemes try to monitor and forecast the traffic by using the recorded history trajectory data of vehicles equipped with GPS devices. The index based schemes construct an index by adopting the trajectory data of the vehicles [5, 6]. And then the routes are recommended according to the history trajectory data of the related vehicles. The clustering based schemes generate the density routes of the road networks by analyzing the trajectory data of vehicles [9, 13, 16, 17]. Reference [1] proposed the MPR scheme for discovering the popular route between two locations by observing the traveling behaviors of many previous users. Reference [18] studied the problem of finding reasonable alternative routes in road networks. In NETSCAN scheme [13], the density routes of the road networks are evaluated by considering both the location and time of the vehicles.

According to the trajectory data, the number of the vehicles within a specific road segment and time period can be used to identify the density routes of a road. However, the existing schemes are not suitable for real road networks. There are three major problems of the existing schemes:

(1) the directions of the roads in the road networks are not considered; (2) the widths and lengths of the road segments are not considered; and (3) the average moving speed of vehicles within a road segment is not considered. In the real road network environments, each road is divided into two directions: positive direction and negative direction. The vehicles in the road toward different directions do not affect each other. Therefore, the congested routes are inaccurate if the directions of the road are not considered. The width and length of each road segment are different in a road network, which will also affect the accuracy of the congested routes. Furthermore, the average moving speed of vehicles within a road segment can identify the congestion of the road.

To overcome these problems, we propose a congested routes discovering scheme, in which the directions, width, and length of roads are considered for congested route discovering in real road network environments. The proposed scheme divides the roads into segments with different widths and lengths. And then, the congested road segments are extracted by considering the average moving speed of the vehicles and the saturation degree of each road segment in the road networks. Finally, we perform clustering schemes to compute the final congested routes in the whole road networks.

The remainder of the paper is organized as follows. We will discuss related work in Section 2. Section 3 presents the details of the proposed scheme. Section 4 contains experimental evaluation that demonstrates the superiority of our proposed scheme. Finally, Section 5 concludes this paper.

2. Related Work

Discovering hot routes or popular routes is a very important technique to support location-based service in road network. Reference [1] studied the discovering scheme of the most popular route (MPR) between two locations by observing the traveling behaviors of many previous users. Reference [1] presented an algorithm to establish the transfer network model for a collection of historical trajectories and utilized the absorbing Markov chain model to derive the transfer probability for transfer nodes. Maximum probability product algorithm is used for discovering the MPR from a transfer network based on the popularity indicators in a breadth-first scheme. Reference [16] defined a hot route which is a general path in the road network containing heavy traffic and studied the discovering scheme of hot routes. Reference [16] proposed a new density-based algorithm called FlowScan. It is a robust algorithm that can handle the complexities in the data and was verified through extensive experiments. Instead of clustering the moving objects, road segments are clustered based on the density of common traffic they share. Reference [15] studied the problem of vehicular traffic density estimation, utilizing the information cues present in the cumulative acoustic signal acquired from a roadside-installed single microphone.

Vehicles which are located in a congested area try to move to a noncongested area. Reference [10] proposed a route discovery method for alleviating traffic congestions to provide a driving route whose trip time becomes short. The proposed method does not need global traffic information but regional traffic information for each vehicle. The vehicle calculates a route for a destination where a summation of evaluation values for roadway segments in the route becomes minimal. Given a spatial range and a user preference of depth/breadth specified by a user, [11] processed a pattern-aware trajectory search (PATS) to retrieve the top K trajectories passing through popular ROIs. PATS support trip planning without requiring prior knowledge of ROIs in the specified spatial range. PATS used a user movement graph to capture travel patterns hidden in trajectories and develop an algorithm to determine the attractive scores of the ROIs and proposed an algorithm BTS for efficiently retrieving the top K trajectories.

Reference [19] proposed a fast path algorithm of finding the best shortest paths in the road network to solve the path planning problem in route guidance systems in terms of accuracy and speed. Reference [20] proposed an adaptive fastest path algorithm capable of efficiently accounting for important driving and speed patterns mined from a large set of traffic data. Reference [20] presented a routing algorithm which uses the road hierarchy and precomputed areas to limit the search space. This improves trip duration by using upgraded roads whenever beneficial and finds routes that take into consideration both speed and driving patterns.

Reference [13] proposed a scheme for discovering dense routes by clustering similar road sections according to both traffic and location in each time period. Reference [13] presented NETSCAN which carries out the clustering of dense sections and incorporates them by forming dense routes. NETSCAN cluster the road sections based upon the network density statistics. This clustering takes into account the orientation of the trajectory. Besides, this method utilizes the network topology to create relevant clusters. To propose a model to assess the evolution for dense route pairs at two consecutive time intervals, DENSITYLINK algorithm is presented. DENSITYLINK allows the characterization of the evolution of the dense road network. Reference [17] proposed a time-based clustering algorithm called Tk-means that adapts the k-means algorithm for trajectory data. Tk-means cluster the objects based on the time intervals of different trajectory's motions. If an object spans different time intervals, it will eventually belong to different clusters. Tk-means used two approaches, an exact method and an approximate method. The exact method computes the actual clusters visited by the object throughout its life time and the approximate method exactly computes some of the actual visited clusters and, based on those computed clusters along with the clusters generated from the remaining data set, it predicts the future motion pattern of the query object.

3. The Proposed Scheme

3.1. Data Model. We assume that the road network is represented by a graph $G(N, E)$, where N denotes the node which is the intersection between different road segments and E denotes the edge which is used to connect two adjacent nodes

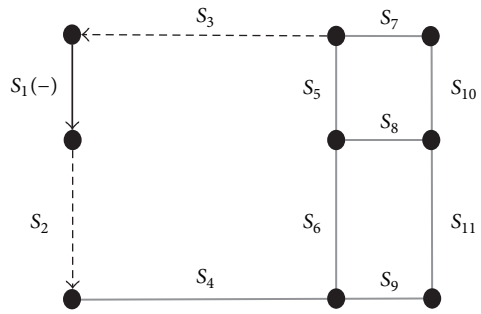


Figure 1: The data model of road network.

in the road network. The trajectory of a vehicle is represented by Tr. Each node N_i in the road network is represented by a point $\{x_i, y_i\}$. E_i denotes a segment of the road network. "+" and "−" are used to represent the different directions of vehicles in a road network. Moreover, since the length and the number of lane of each road are different, the length and width of each road segment are stored. Therefore, each road segment is represented by $S_i(\pm) = \{N_i, N_j, \text{length}, \text{width}\}$, where length is the length of a road segment and width is the number of traffic lanes. As shown in Figure 1, S_2 and S_3 are the neighbor segments of S_1 in a road network G.

In a road network G, each road segment S_i stores the information of its directly connected road segments. This information is used for the following clustering evaluations. Since the vehicles may move continuously or stay in a position, it is necessary to have the location knowledge of each vehicle according to the timestamps. Suppose that the trajectory Tr of each vehicle is as follows:

$$\text{Tr}_n = \langle (S_1(\pm), T_1), (S_2(\pm), T_2), \ldots, (S_k(\pm), T_k) \rangle, \quad (1)$$

where S_i denotes the segment ID and T_i is the timestamp. According to T_i, the location of each vehicle can be retrieved easily.

3.2. Congested Road Segment. The initial road information and trajectory data can be used to determine the existence of vehicles in each road segment of different directions. The complexity value of each road segment is evaluated. The road segment is considered as congested region if the evaluated complexity value is higher than the predefined threshold value. The clustering algorithm is performed among congested road segments. The road segments with low moving speed and high number of vehicles are determined as congested road segments. Figure 2 shows the procedure of computing congested routes.

In this paper, the congested road segments are computed according to the different directions of the roads. The location and direction of each vehicle can be retrieved from the recorded trajectory data. The complexity value of each road segment is computed by considering the average speed of the vehicles in the road segment and the saturation degree of the road segment. The fast moving speed indicates that the congestion of the road segment is low. In contrast, the low moving speed indicates that the congestion of the road

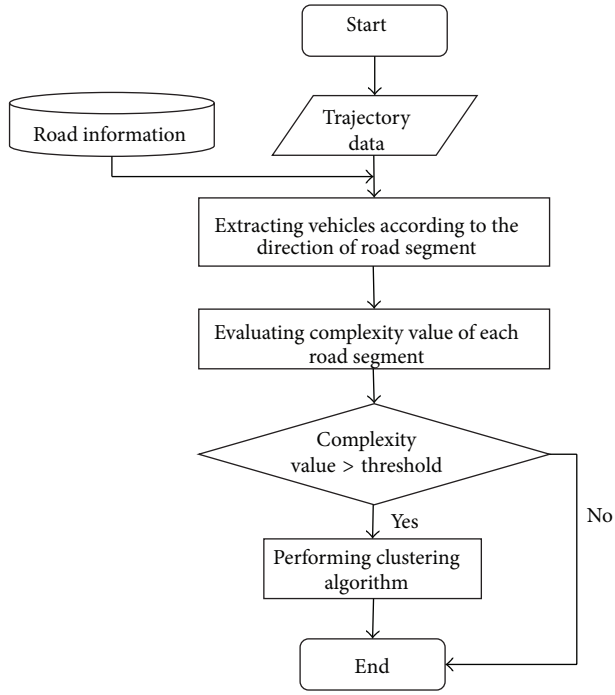


Figure 2: The procedure of computing congested routes.

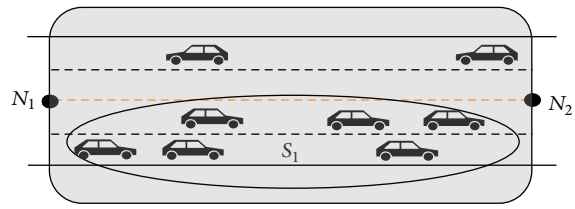


Figure 3: The road segment between nodes N_1 and N_2 in a road network.

segment is high. The saturation degree is computed based on the number of the vehicles within a road segment and the length and width of a road segment, which are indicated in Figure 3. We define that the congested road segments within a road network are the road segments with high complexity values.

The average moving speed (Av) of the vehicles in a road segment according to different directions is computed by the following equation (2), where $V(Ob_i)$ denotes the moving speed of a vehicle Ob_i. The saturation (Sat) according to the width (S_{width}) and length (S_{length}) of a road segment is computed in (3), where Ob_n denotes the number of the vehicles in a road segment. As a result, the complexity value of a road segment is computed by (4) which combines (2) and (3); α denotes the weight value between the average moving

Congested routes detection algorithm
Input:
Set of road segment list $S = \{S_1, S_2, \ldots, S_{n+1}\}$
Set of trajectory $\mathrm{Tr} = \{\mathrm{Tr}_1, \mathrm{Tr}_2, \ldots, \mathrm{Tr}_n\}$
Set of time interval $T = \{T_1, T_2, \ldots, T_n\}$
Threshold β—trajectory velocity and road weight
Output:
Threshold α—road density
Set of cluster groups $\mathrm{CH} = \{\mathrm{CH}_1, \mathrm{CH}_2, \ldots, \mathrm{CH}_n\}$
CH ← Initialization
for every time interval t
while there exist Tr in segment list S
for each satisfied α in S
segment S = create candidate c
end for
if exist neighbor segment N in candidate c
create CH ← extend from c to N
else if
create CH ← candidate c
end if
end while
end for

Algorithm 1: The algorithm of the proposed scheme.

speed of vehicles and the saturation of a road segment. Consider

$$\mathrm{Av}_i(\pm) = \frac{\sum_{i=1}^{n} V(Ob_i)}{Ob_n(\pm) \times V_{\max}}, \tag{2}$$

$$\mathrm{Sat}_i(\pm) = 1 - \frac{Ob_n(\pm)}{S_{\mathrm{width}} \times S_{\mathrm{length}}}, \tag{3}$$

$$Ri_i(\pm) = \alpha \times \mathrm{Av}_i(\pm) + (1 - \alpha) \times \mathrm{Sat}_i(\pm). \tag{4}$$

3.3. Congested Routes Detection. In this section, we present the algorithm of congested routes detection. The algorithm operates in two phases. In the first phase, the complexity value of each road segment in the road network according to different directions is computed. In the second phase, the congested routes of a road network are evaluated by clustering the congested road segments with each time interval. When the complexity value of a road segment is larger than the predefined threshold value, the road segment is considered as a congested road segment. Finally, the congested road segments with same direction are clustered together. Algorithm 1 shows the congested routes detection algorithm.

Since the complexity values of road segments are changed according to different timestamps, they have to be computed periodically. The congested routes of a road network are computed according to the complexity values. Figure 4 shows the congested routes (the dotted areas) of a road network in different timestamp T. According to the recorded trajectory data of vehicles at time $T = 0$, the congested routes of the road network of different directions are generated, such as $S_2(+)$ and $S_5(-)$ in Figure 4(a). As shown in Figure 4(b), when time $T = 1$, $S_1(+)$, $S_5(-)$, and $S_6(-)$ are evaluated as congested road segments. Since $S_5(-)$ and $S_6(-)$ are neighbor road segments and have the same direction in the road network, they are clustered together.

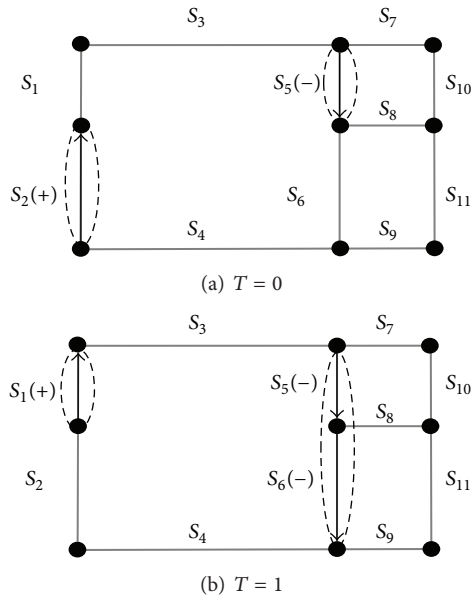


Figure 4: The clusters according to different timestamps.

4. Performance Evaluation

In this section, we introduce the performance evaluation by comparing the proposed scheme with the existing scheme

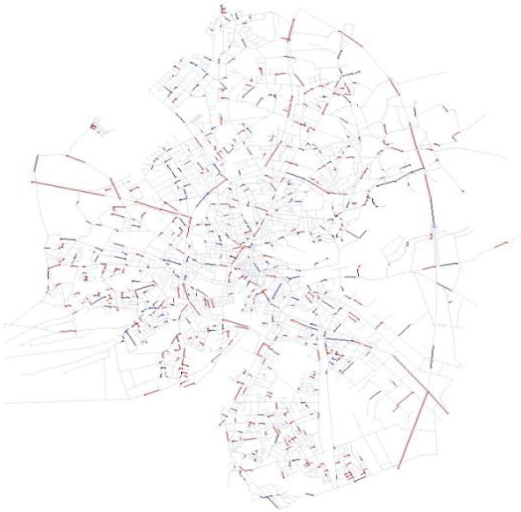


Figure 5: The congested route of Oldenburg city.

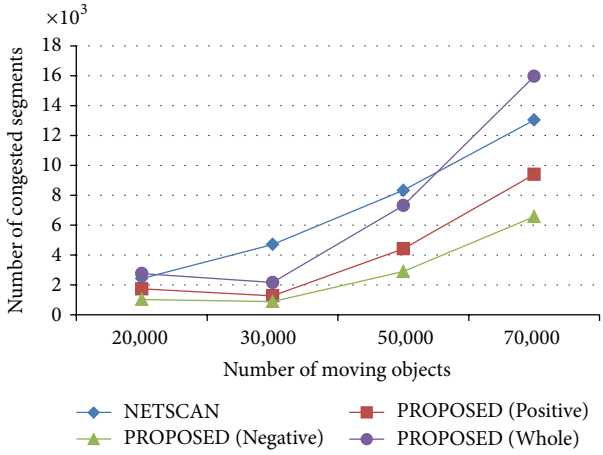


Figure 6: The number of congested routes according to the number of vehicles.

NETSCAN [13]. The vehicles are generated by the network-based generator [21]. The complexity values and clusters are generated according to the number of vehicles in each time interval. All of the experiments are coded in Java and the experiments are performed in Intel i3 3.0 GHz CPU and 4 G memory. Table 1 summarizes the parameters for this performance evaluation.

In the first experiment, we show the congested routes road networks of Oldenburg city by using our proposed scheme. In this experiment, the total number of vehicles in the road network is set to 50,000 and the saturation of the road is set to 30%. As shown in Figure 5, the results indicated that the congested routes of the road network are different according to the different directions of the road networks. The blue and red regions represent the congested routes of the road networks in positive direction and negative direction, respectively.

In Figure 6, we compare the NETSCAN scheme with our proposed scheme. The number of the congested routes of

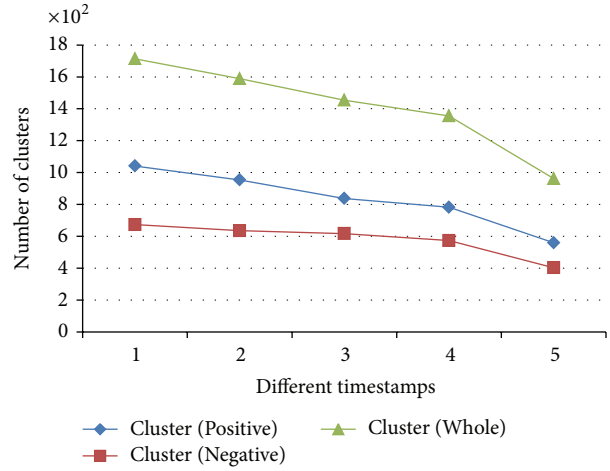


Figure 7: The number of congested routes according to the different timestamps.

Table 1: The values of parameters.

Parameter	Value
Road network	Oldenburg city
The number of segments	7,035
The number of nodes	6,105
The number of vehicles	10,000~100,000
Velocity	0~120

NETSCAN and the proposed scheme are evaluated according to the number of the vehicles. For the proposed scheme, the congested routes are evaluated in different directions (positive direction and negative direction) and same direction, respectively. PROPOSED (Positive) and PROPOSED (Negative) mean the number of congested routes of each direction of road segments, and PROPOSED (Whole) means the number of congested routes of bidirectional road segments according to the number of vehicles. The results show that the number of the congested routes is increased when the number of the vehicles increases. The number of the congested routes of the proposed scheme is similar when the number of the vehicles is between 20,000 and 30,000. This is because the saturation of each road segment is considered in the proposed scheme. When the width and length of a road segment are large, 20,000 and 30,000 vehicles are not large for the road. Therefore, most of the road segments are not identified as congested routes at first. For NETSCAN scheme, the number of congested routes is increased proportionally with the increase of the number of vehicles.

Figure 7 shows the number of congested routes according to the various timestamps when the time interval is set to 1 hour. The congested routes are evaluated in different directions (positive direction and negative direction) and same direction, respectively. Cluster (Positive) and Cluster (Negative) mean the number of congested routes of each direction of road segments according to the different timestamps. We can see that the number of the congested routes of the positive direction is larger than that of the negative

direction. And the number of the congested routes of the proposed scheme that does not consider the direction of the road segment is larger than that of the congested routes of the proposed scheme considering the direction of the road segment.

5. Conclusion

In this paper, we have proposed a congested routes discovering scheme in real road networks. The proposed scheme divides the road into segments with different widths and lengths. It extracts the congested road segments based on the average speed of the vehicles and the saturation degree of a road segment. The final congested routes are computed by performing clustering scheme. The experimental results have shown that the proposed scheme can discover the congested routes in different directions over the existing schemes. In the future, we will show the superiority of our approach by using the real trajectory data of vehicles.

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

Acknowledgments

This research was supported by the MSIP (Ministry of Science, ICT and Future Planning), Korea, under the ITRC (Information Technology Research Center) Support Program (NIPA-2014-H0301-14-1022) supervised by the NIPA (National IT Industry Promotion Agency) and the C-ITRC (Convergence Information Technology Research Center) Support Program (NIPA-2014-H0401-14-1007) supervised by the NIPA (National IT Industry Promotion Agency), by the ICT R&D Program of Discovery Platform for Large-Scale Real Time Data Analysis, MSIP/IITP (14-824-09-001, Development of High Performance Visual Big Data Discovery Platform for Large-Scale Realtime Data Analysis), and by the National Research Foundation of Korea (NRF) Grant funded by the Korean Government (MSIP) (no. 2013R1A2A2A01015710).

References

[1] Z. Chen, H. T. Shen, and X. Zhou, "Discovering popular routes from trajectories," in *Proceedings of the IEEE 27th International Conference on Data Engineering (ICDE '11)*, pp. 900–911, Hanover, Germany, April 2011.

[2] P. Cudre-Mauroux, E. Wu, and S. Madden, "TrajStore: an adaptive storage system for very large trajectory data sets," in *Proceedings of the 26th IEEE International Conference on Data Engineering (ICDE '10)*, pp. 109–120, Long Beach, Calif, USA, March 2010.

[3] E. Kanoulas, Y. Du, T. Xia, and D. Zhang, "Finding fastest paths on a road network with speed patterns," in *Proceedings of the 22nd International Conference on Data Engineering*, p. 10, April 2006.

[4] G. Gidófalvi, C. Borgelt, M. Kaul, and T. B. Pedersen, "Frequent route based continuous moving object location- and density prediction on road networks," in *Proceedings of the 19th ACM SIGSPATIAL International Conference on Advances in Geographic Information Systems (GIS '11)*, pp. 381–384, November 2011.

[5] J.-W. Chang, M.-S. Song, and J.-H. Um, "TMN-tree: new trajectory index structure for moving objects in spatial networks," in *Proceedings of the IEEE 10th International Conference on Computer and Information Technology (CIT '10)*, pp. 1633–1638, Bradford, UK, June-July 2010.

[6] M. Huang, P. Hu, and L. Xia, "A grid based trajectory indexing method for moving objects on fixed network," in *Proceedings of the 18th International Conference on Geoinformatics*, June 2010.

[7] J.-I. Won, S.-W. Kim, J.-H. Baek, and J. Lee, "Trajectory clustering in road network environment," in *Proceedings of the IEEE Symposium on Computational Intelligence and Data Mining (CIDM '09)*, pp. 299–305, April 2009.

[8] G.-P. Roh, J.-W. Roh, S.-W. Hwang, and B.-K. Yi, "Supporting pattern-matching queries over trajectories on road networks," *IEEE Transactions on Knowledge and Data Engineering*, vol. 23, no. 11, pp. 1753–1758, 2011.

[9] N. Pelekis, I. Kopanakis, E. E. Kotsifakos, E. Frentzos, and Y. Theodoridis, "Clustering trajectories of moving objects in an uncertain world," in *Proceedings of the IEEE International Conference on Data Mining (ICDM '09)*, pp. 417–427, December 2009.

[10] M. Kimura, S. Inoue, Y. Kakuda, and T. Dohi, "A route discovery method for alleviating traffic congestion based on VANETs in urban transportations considering a relation between vehicle density and average velocity," in *Proceedings of International Symposium on 10th International Symposium on Autonomous Decentralized Systems (ISADS '11)*, pp. 299–302, March 2011.

[11] L.-Y. Wei, W.-C. Peng, and W.-C. Lee, "Exploring pattern-aware travel routes for trajectory search," *ACM Transactions on Intelligent Systems and Technology*, vol. 4, no. 3, article 48, 2013.

[12] Y. Xu and J. Wang, "Optimal path solution of urban traffic road," in *Proceedings of the 7th International Conference on Natural Computation (ICNC '11)*, pp. 799–802, July 2011.

[13] A. Kharrat, K. Zeitouni, I. Sandu-Popa, and S. Faiz, "Characterizing traffic density and its evolution through moving object trajectories," in *Proceedings of the 5th International Conference on Signal Image Technology and Internet Based Systems (SITIS '09)*, pp. 257–263, December 2009.

[14] K. W. Min, J. W. Kim, and J. H. Park, "Optimal route determination technology based on trajectory querying moving object database," in *Proceedings of International Conference on Database and Expert Systems Applications*, pp. 666–675, 2006.

[15] V. Tyagi, S. Kalyanaraman, and R. Krishnapuram, "Vehicular traffic density state estimation based on cumulative road acoustics," *IEEE Transactions on Intelligent Transportation Systems*, vol. 13, no. 3, pp. 1156–1166, 2012.

[16] X. Li, J. Han, J. Lee, and H. Gonzalez, "Traffic density-based discovery of hot routes in road networks," in *Proceedings of SIAM International Conference on Data Mining*, pp. 441–459, 2007.

[17] H. M. O. Mokhtar, O. Ossama, and M. E. Sharkawi, "A time parameterized technique for clustering moving object trajectories," *Journal of Data Mining and Knowledge Management Process*, vol. 1, no. 1, pp. 14–30, 2011.

[18] I. Abraham, D. Delling, A. V. Goldberg, and R. F. Werneck, "Alternative routes in road networks," *Journal of Experimental Algorithmics*, vol. 18, article 1.3, 2013.

[19] A. Selamat, M. Zolfpour-Arokhlo, S. Z. Hashim, and M. H. Selamat, "A fast path planning algorithm for route guidance system," in *Proceedings of the IEEE International Conference on Systems, Man, and Cybernetics (SMC '11)*, pp. 2773–2778, Anchorage, Alaska, USA, October 2011.

[20] H. Gonzalez, J. Han, X. Li, M. Myslinska, and J. P. Sondag, "Adaptive fastest path computation on a road network: a traffic mining approach," in *Proceedings of International Conference on Very Large Data Bases*, pp. 794–805, 2007.

[21] T. Brinkhoff, "A framework for generating network-based moving objects," *GeoInformatica*, vol. 6, no. 2, pp. 153–180, 2002.

Hindawi Publishing Corporation
Advances in Multimedia
Volume 2015, Article ID 960416, 9 pages
http://dx.doi.org/10.1155/2015/960416

Research Article

Study on Strengthening Plan of Safety Network CCTV Monitoring by Steganography and User Authentication

Jung-oh Park[1] and Sanggeun Kim[2]

[1]*Department of Information Communications, Dongyang Mirae University, Seoul 152-714, Republic of Korea*
[2]*Division of Computer Engineering, Sungkyul University, Anyang-si 430-742, Republic of Korea*

Correspondence should be addressed to Sanggeun Kim; sgkim@sungkyul.edu

Received 16 October 2014; Accepted 4 December 2014

Academic Editor: Seungmin Rho

Copyright © 2015 J.-o. Park and S. Kim. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Recently, as the utilization of CCTV (closed circuit television) is emerging as an issue, the studies on CCTV are receiving much attention. Accordingly, due to the development of CCTV, CCTV has IP addresses and is connected to network; it is exposed to many threats on the existing web environment. In this paper, steganography is utilized to confirm the Data Masquerading and Data Modification and, in addition, to strengthen the security; the user information is protected based on PKI (public key infrastructure), SN (serial number), and *R value* (random number) attributed at the time of login and the user authentication protocol to block nonauthorized access of malicious user in network CCTV environment was proposed. This paper should be appropriate for utilization of user infringement-related CCTV where user information protection-related technology is not applied for CCTV in the future.

1. Introduction

Due to networking of CCTV and openness of the internet, the necessity to protect privacy video data and information safety, trust, protection, and concealment is in demand, and as the according application technique, the study on steganography method which inserts confidential information to the transfer media is actively in progress.

The existing web has much vulnerability, and as CCTV was involved with networking, it became a problem that CCTV is exposed to such vulnerability of web. Also, CCTV videos are related to privacy, and if such videos are exposed to unspecified public, it would be a sufficiently sensitive issue.

Recently, there are many problems related to CCTV; the manager does not frequently change the public IP or dynamic IP of network camera, rendering it easy to be exposed outside, and once IP address is leaked, the crack program breaking the password is used to access the administrator account and have the monitoring video leaked at any time. Network monitoring camera, however, has a large data size and sends data through streaming unlike other IT resources; thus it is hard to change the IP address and is easily exposed outside. Due to such issues, it is only a matter of time for the monitoring video to be leaked. Other than that, there is possibility of leakage of CCTV videos due to several threats, and data security must be provided accordingly. Existing studies [1–17] on CCTV security concentrated on security structure of CCTV network infrastructure, security policy, and utilization under specific environment (crime prevention, etc.). This paper shifts from such general topics to propose a user authentication protocol under network CCTV environment which reinforces CCTV monitoring with steganography and prevents malicious user access. International trends of CCTV security are given in Table 1.

2. Related Studies

2.1. Network CCTV System. By inserting IP to the existing CCTV, CCTV can be managed individually, and as long as internet is available, remote management and remote monitoring are available. Such network CCTV system is as in Figure 1.

Table 1: International trends of CCTV security (purpose and characteristics).

Country	Purpose	Location	Characteristics
Korea	Theft prevention, traffic and parking, and disaster prevention	All regions of Korea	Operating integrated CCTV control centers by local governments around the nation
UK	Theft prevention and prevention of riot, protest, and terrorism	All regions of UK	Converted from analog to HD CCTV, installing large number of CCTV compared to population
Germany	Building security such as alert on theft, fire, intrusion, and robbery	Major buildings	Video equipment related to theft and intrusion combined as one
UAE	Prevention of terrorism and various crimes	Facilities such as schools, hospitals, and parks	Entirely relies on importation with high ratio of CCTV used to prevent auto theft
United States	Public security such as homeland security and disaster prevention	All regions of the United States	Has largest market size and quickly applies latest technological trends (intelligent CCTV)
Switzerland	Homeland security, public security, and corporations	Major public institutions	High ratio of CCTV used to maintain public order
China	Crime prevention and public security	Major public institutions, automobiles, and households	Low ratio of HD CCTV and low availability

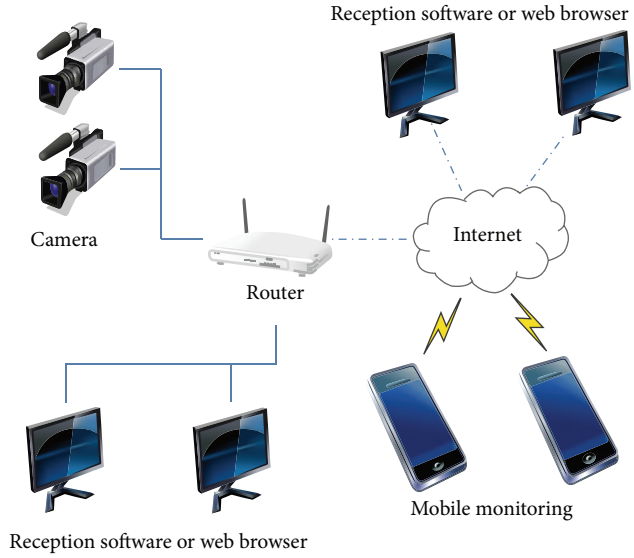


Figure 1: Network CCTV system.

2.2. Problems of Network CCTV Systems. As CCTV gets involved with networking, there are many emerging issues. The number of police protecting the safety of the citizens is increasing every year, but due to the increase in social violent crime occurrences and public order issues, the installation/operation of network-based CCTV systems are expanding nationwide for the purpose of citizen protection and personal security. Particularly, thanks to the advancement of internet technologies, the utilization scope became more diverse from illegal trash dumping to public order/crime prevention to illegal parking/stop, and so forth.

On the other hand, despite the expansion of installation/expansion of CCTV system, relative absence of clear governmental guidelines and reckless introduction with standards are emerging as security issues [18, 19].

The purpose of CCTV in different nations is prevention of major crimes and promotion of public security. Existing analog CCTV devices are changing into network-based digital CCTV with HD screen. The market for network-based CCTV system is growing for operation of integrated control centers. Examples [20–22] of security scenarios that can occur in network-based CCTV systems are as follows.

① Collection of information by CCTV system that uses public IP: as the system is linked to various paths, exposure of IP address as problem that information on the operating system and application used by CCTV system server can be collected with ease.

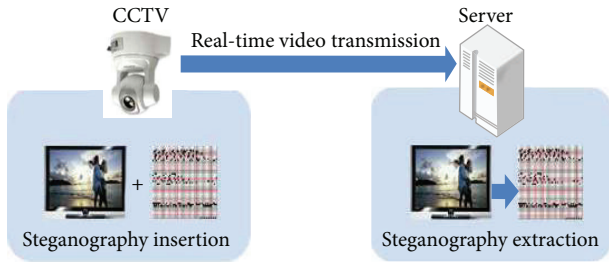


Figure 2: Overall structural diagram.

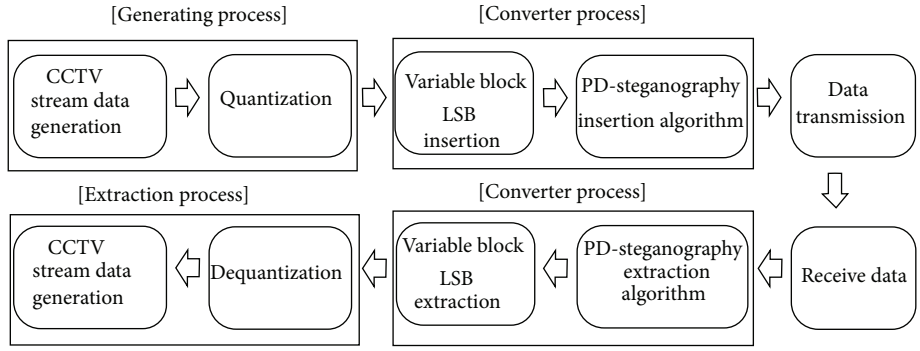


Figure 3: Overall data flowchart.

Hackers can use this as a starting point to make different hacking attempts based on information collected from each server.

② Sniffing and spoofing of sections with security vulnerabilities: since all IP-based CCTV systems communicate via different network devices and servers in a public network, information can be exposed when a section without security infrastructure is hacked.

③ Lack of data safety from nonapplication of encryption on video data: existing analog CCTV and network CDTV with relatively low hardware specifications have a problem in which real-time data cannot be encrypted. This results in easy exposure of data stored in servers.

④ Security vulnerabilities of CCTV control centers: as control centers are always connected to network because they need to manage and control CCTV on a real-time basis, security vulnerabilities of server and control PC can expose ID and password of important administrator accounts. Hacked CCTV systems can be used as a means to attack internal infrastructure and attack route.

As shown in the hacking scenarios described above, hacking of important information and exposure of CCTV information have reached a dangerous level of security alert for network CCTV systems resulting in leakage of confidential information of public institutions and corporations, deletion or alteration of important information such as major theft crimes, and unauthorized release of private CCTV information.

3. Video Steganography Application Plan for Network CCTV Monitoring Security

As in Figure 2, the overall system structure diagram shows that when sending the video from the CCTV, the steganography is inserted realtime before being sent to the server, and then the server extracts the steganography from the video again.

This report proposes a method to protect the system by inserting steganography to the real-time video of CCTV monitoring system provided in open source. Figure 3 is the overall data flowchart of this report. This structure is in three different work processes of generation, conversion, and extraction. The generation part generates the video data from CCTV and converts the video data into bits. The conversion part is the LSB process for the bit-converted video data and proposed steganography insertion application. The extraction part is the process of reverse-quantization of data extract by LSB method and generating video data. The proposed steganography input method is as in Figure 4.

Figure 5 shows the application of shift to the corresponding data line by the same rule as in Table 2. For example, the data in Figure 4 shall have the time value of image filmed with CCTV, user name, key value of CCTV, and so forth.

4. User Authentication Protocol to Block Malicious User

Figure 6 is the overall outline diagram of the proposed protocol. In the proposed user registration process, along with the user authentication, the user and related CCTV are

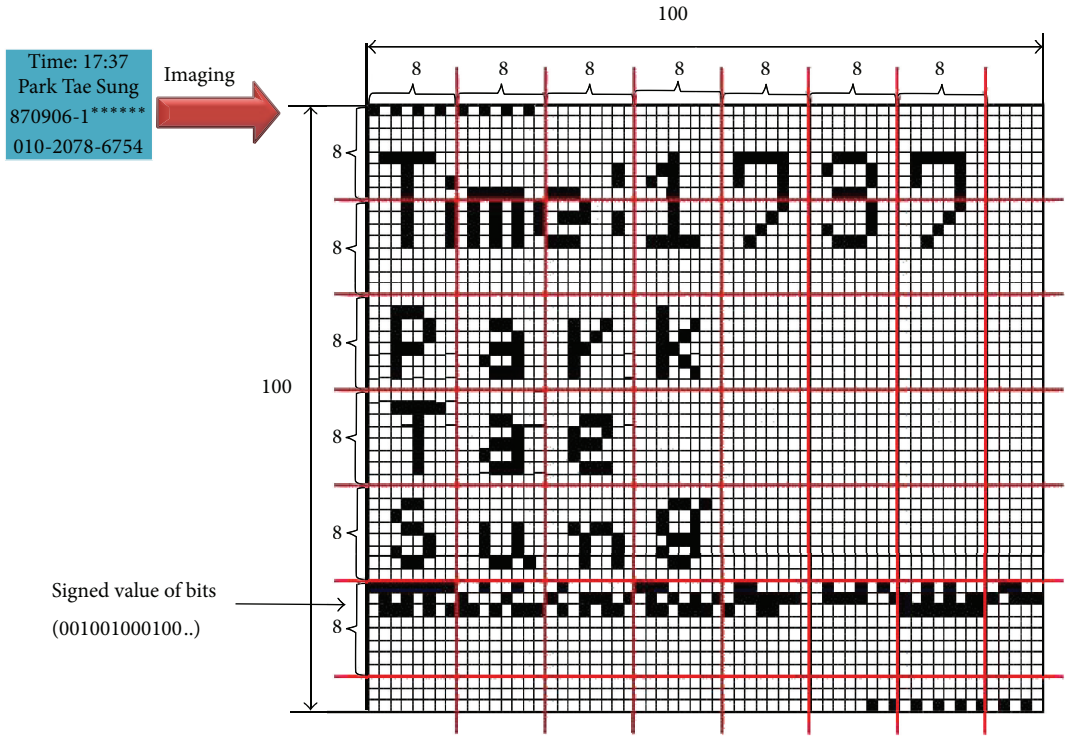


Figure 4: After shift of steganography-inserted data.

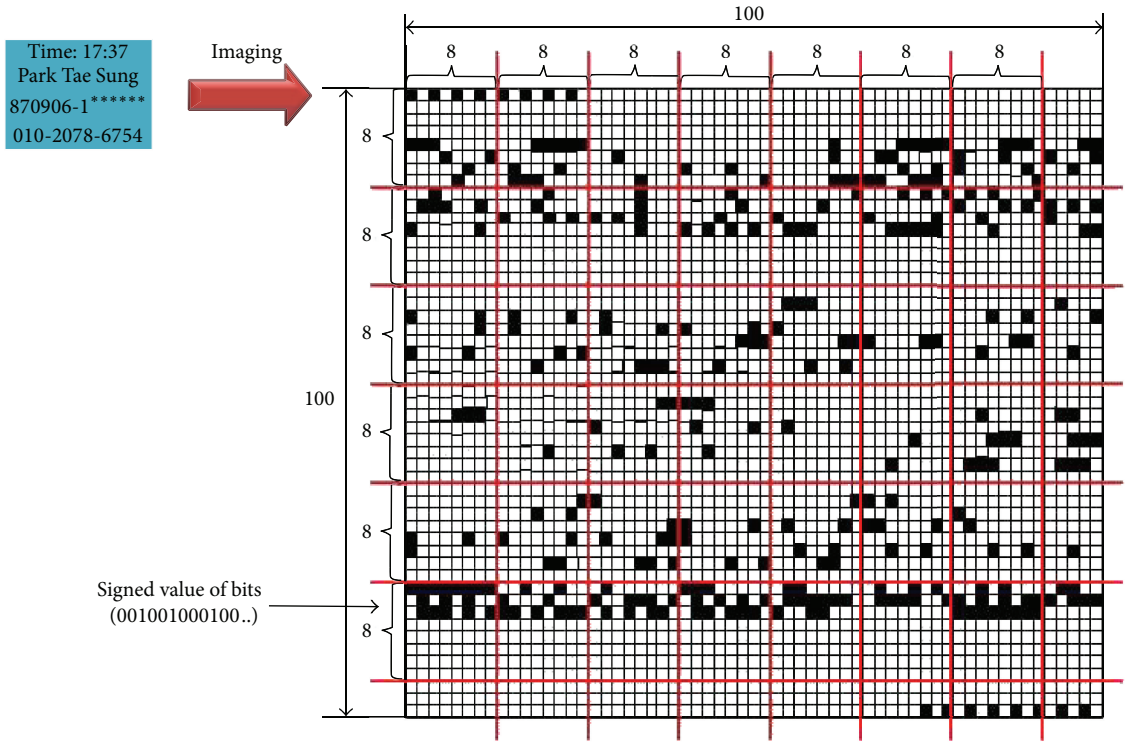


Figure 5: Before shift of steganography-inserted data.

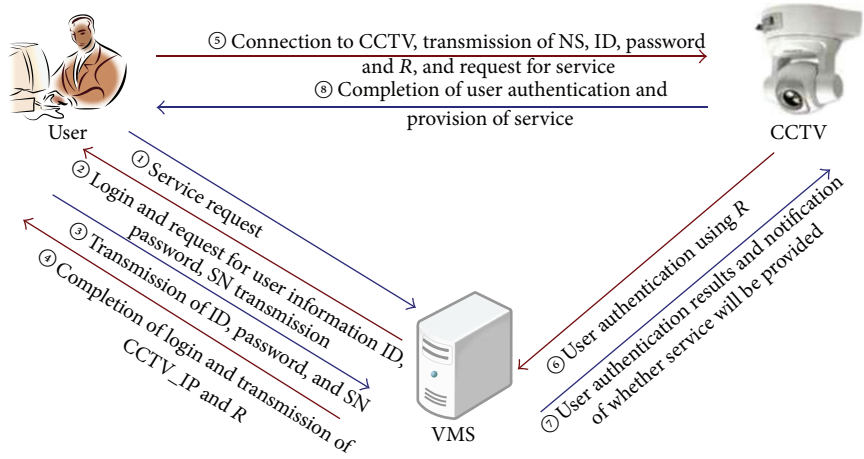


Figure 6: Overall composition diagram.

Table 2: Steganography data shift rules.

Line	Shift
1	None
2	$\gg 1$
3	$\gg 3$
4	$\gg 6$
5	$\gg 10$
⋮	⋮
n	$\gg n(n-1)/2$

synchronized at the same time providing the SN of CCTV, and in user authentication process, this SN and random number attributed to the user are used to strengthen identity authentication, and it is rendered impossible to leak CCTV video by password unlock crack or simple CCTV IP access.

4.1. User Registration Protocol. Figure 7 is the user registration process of the proposed protocol. The proposed user registration protocol is achieved by executing the following procedure.

① The user sends the network CCTV video service request message to the operation PC of VMS.

② The operation PC of VMS requests the user information necessary for member subscription.

③ The user requests the user information for member subscription.

Response {User Data(Name, Num)}.

The corresponding information is, respectively, user's name and user's resident registration number.

④ The operation PC of VMS sends the received user information to the identity confirmation agency and requests authentication.

Verify User Data confirm {User(Name, Num)}.

VMS does not feature an agency to identify the information for the user. Therefore, the operation PC of VMS sends the data received from the user to the identity confirmation agency to request the confirmation of the information for the user.

⑤ The identity confirmation agency checks the user's personal information, and if the information is correct, it sends an approval message to the operation PC of VMS, and if not, it sends a rejection message.

⑥ The operation PC of VMS sends the response message received from the identity confirmation agency to the authentication server.

⑦ The operation PC of VMS checks the user information with the received message.

⑧ The authentication server sends the approval message for the user information to the operation PC.

⑨ The operation PC sends the approval message received from the authentication server to the user.

⑩ The user encrypts the ID and password to be used with the public key of VMS and sends it to the operation PC of VMS.

Send $\{E_{VMS_{Pu}}(ID \parallel PW)\}$.

The user sends the ID and password encrypted with the public key of VMS so that the user ID and password can only be decrypted by VMS and it is safe from external attacks such as password speculation attack.

⑪ The operation PC decrypts the data received from the user with the personal key of VMS to extract ID and password.

Transaction $\{D_{VMS_{Pri}}(ID \parallel PW)\}$.

⑫ The operation PC sends the value hashed to prevent the exposure of user's ID and password to the authentication server.

Send $\{ID \parallel h(PW)\}$.

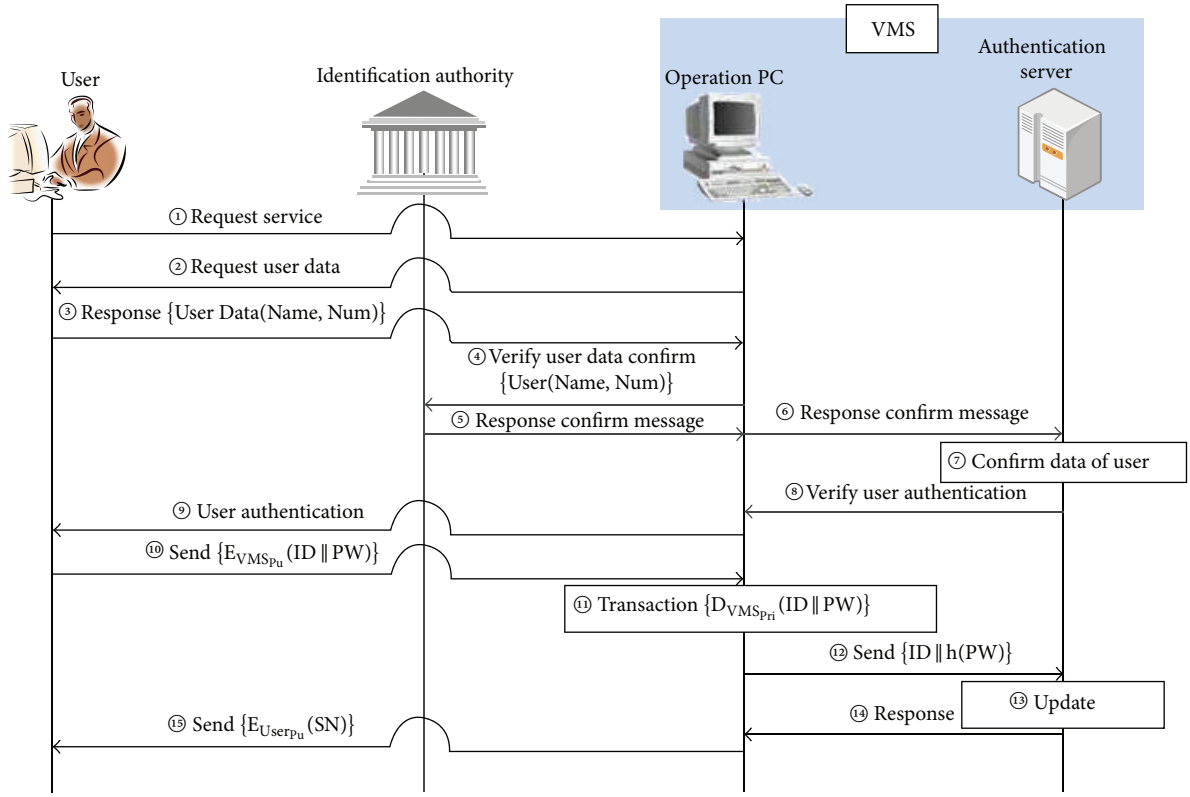


Figure 7: Proposed user registration protocol.

⑬ The authentication server registers the received user information.

⑭ The authentication server sends the result for the completion of member subscription to the operation PC.

⑮ The operation PC encrypts the SN value of CCTV necessary for the authentication process with the public key of the user and sends it.

Send $\{E_{User_{Pu}}(SN)\}$.

The objective of this user registration protocol is to check the user information and obtain SN which is the information needed when requesting service from the network CCTV that the user wants to see.

4.2. User Authentication Protocol. Figure 8 is the proposed user authentication protocol process.

The proposed user authentication protocol is achieved by executing the following procedure.

① The user makes a service request to the operation PC of VMS.

② The operation PC checks the member subscription of the user before providing the service, and if the user is a member, it requests the user information and CCTV SN distributed at the time of member subscription.

③ After encrypting the hashed data of user ID, password, and CCTV SN value with the public key of VMS, it is sent to the operation PC.

Response $\{E_{VMS_{Pu}}(ID \parallel PW \parallel h(SN))\}$.

④ The operation PC decrypts the received data with the personal key of VMS to check the SN value of CCTV and hashes to prevent exposure of user ID and password and sends it to the authentication server.

Send $\{ID \parallel h(PW)\}$.

⑤ The authentication server checks the received ID and password and generates a single-use R value for the corresponding user.

⑥ The authentication server sends the generated R value to the operation PC.

⑦ The operation PC encrypts the corresponding port number of IP information of CCTV for the SN value and R value received from the authentication server together with the public key of the user and sends it to the user.

Send $\{E_{User_{Pu}}(R \parallel CCTV\_IP \parallel P\_Num)\}$.

⑧ The user decrypts the received data with the personal key of the user to access CCTV. The user connects the data where SN of CCTV is encrypted with the public key of CCTV to the data where the user ID,

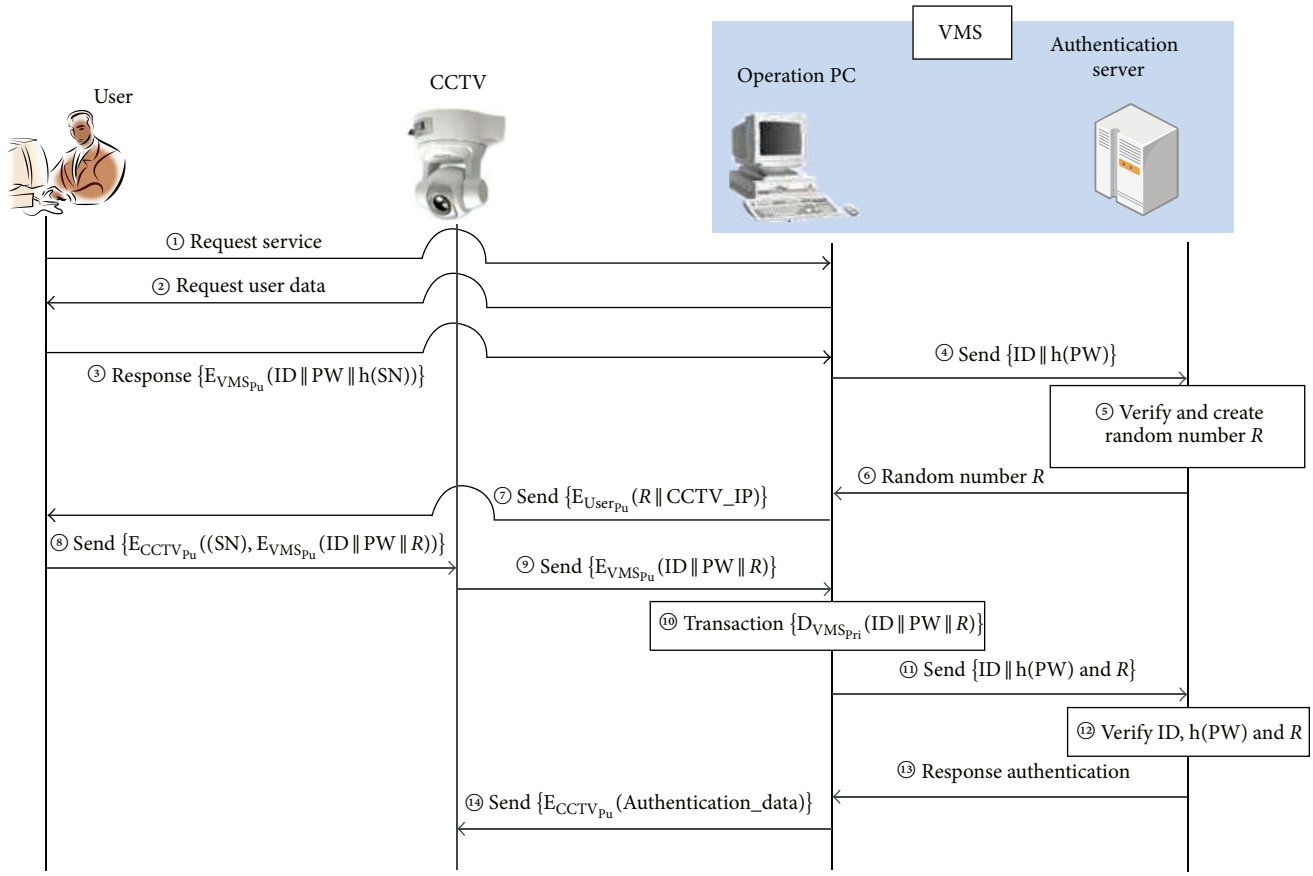


Figure 8: Proposed user authentication protocol.

password, and random number (R) are encrypted with the public key of VMS and sends it to CCTV.

Send $\{E_{CCTV_{Pu}}(SN) \parallel E_{VMS_{Pu}}(ID \parallel PW \parallel R)\}$.

⑨ CCTV decrypts the received data with the personal key of CCTV, and if the SN value matches that of the CCTV itself, it sends the data encrypted with the public key of VMS to VMS.

Send $\{E_{VMS_{Pu}}(ID \parallel PW \parallel R)\}$.

⑩ VMS operation PC decrypts the received data with the personal key of VMS and extracts ID, password, and R value.

Transaction $\{D_{VMS_{Pri}}(ID \parallel PW \parallel R)\}$.

⑪ The operation PC transfers the hash value and random number R to the authentication server in order to prevent exposure of ID and password.

Send $\{ID \parallel h(PW) \parallel R\}$.

⑫ The authentication server verifies that the received ID, password, and R value are the same as those provided by VMS.

Verify ID, h(PW), and R.

⑬ Send user authentication message to the operation PC.

⑭ Operation PC encrypts the user authentication message with the public key of CCTV and sends it to CCTV.

Send $\{E_{CCTV_{Pu}}(Authentication\_data)\}$.

5. Implementation and Performance Evaluation

Figure 9 shows the VMS Client access of the proposed system. It shows the insertion of SN value and R value attributed from the server and the port number, and the server IP is also showing.

The proposed user authentication protocol is used to authenticate the SN acquired by the user when registering the user. In the authentication process, checking SN and comparing information such as R value, ID, and password of the corresponding session render it safe from many threats, and by using the PKI-based encryption mechanism, data confidentiality is guaranteed, and by applying hash algorithm to user's personal information, the personal information is also guaranteed integrity.

Figure 10 shows the photo before and after the insertion of steganography. Through this Figure, it can be shown that there is no visual difference in the video despite the insertion

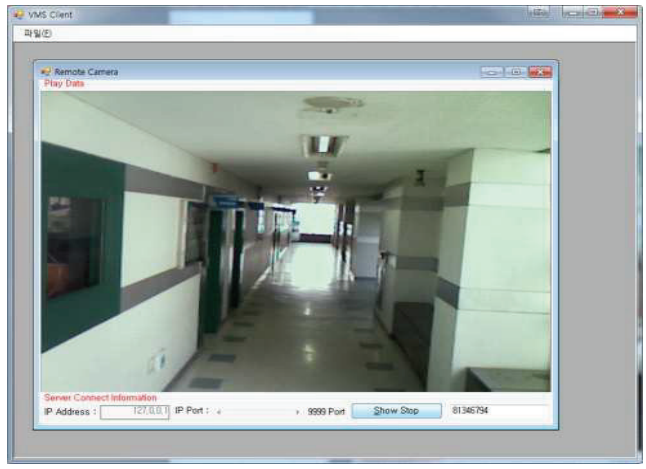


Figure 9: VMS Client implementation.

(a) (b)

Figure 10: Before (a) and after (b) the insertion of steganography.

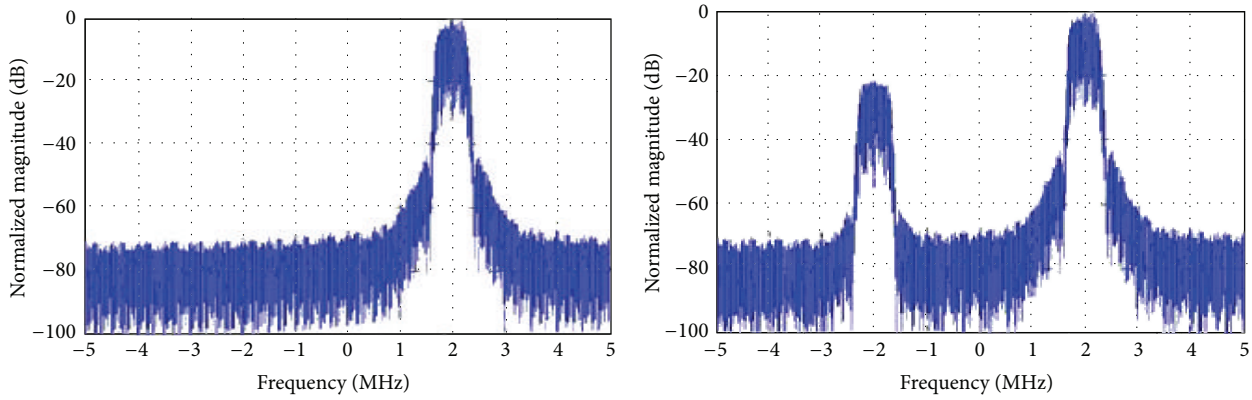


Figure 11: Comparison of frequency before (a) and after (b) the insertion of steganography.

of steganography, and through Figure 11, it is shown that the increase of complexity in data leads to the increase in the strength of encryption.

The safety of the existing network CCTV system environment and the proposed system is as in Table 3.

6. Conclusion and Future Research

In this report, the image checking technique through steganography for security of image transfer process and user authentication protocol to block malicious users in network

Table 3: Comparative analysis of safety.

	No authentication	Existing system	Proposed system
Password speculation attack	Weak	Weak	Safe
User impersonation attack	Weak	Weak	Safe
Replay attack	Weak	Weak	Safe
Omnidirectional safety	Weak	Weak	Safe
Website hacking	Weak	Weak	Safe
Input contents falsification, keyboard hacking	Weak	Weak	Safe

CCTV environment was proposed. In future, it would be necessary to continue to complement weakness for greater safety against attacks of malicious users and search for a more efficient algorithm and authentication method.

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

References

[1] S. Kim, *A Study about Ways to Improve Crime Prevention Effects of Crime Prevention CCTV*, Dongguk University, 2007.

[2] H. No, *Effective Use of CCTV for Crime Prevention*, Korean Association of Public Safety and Criminal Justice, 2004.

[3] E. E. Zelniker, "Global abnormal behaviour detection using a network of CCTV cameras," in *Proceedings of the 8th International Workshop on Visual Surveillance*, Marseille, France, October 2008.

[4] S. Baek, *Design and Implementation of a Video Surveillance System in a Wired/Wireless Network Environment*, Dankook University, Yongin, Republic of Korea, 2006.

[5] C. Im, *A Study on the Problems with the Use of CCTV for Crime Prevention and Ways for Improvement*, Yonsei University, 2007.

[6] Y. Shin, "A study on the protection of personal information following the introduction of CCTV at public institutions," *Journal of Korean Association for Regional Information Society*, vol. 11, no. 2, pp. 1–21, 2008.

[7] I. Minhyeok, "The direction of crime prevention policies through analysis of the crime prevention effects of crime prevention CCTV," *Korean Political Science Association*, vol. 12, no. 4, pp. 77–101, 2008.

[8] S. Go, "A study on human rights infringement and likelihood of risks when CCTV video images are stored long term indiscriminately," *Internet Law*, vol. 27, pp. 49–72, 2005.

[9] Y. Kim, *The Current State of Development of IP Cameras, Storage Solutions and Video Analysis*, Korea Educational Center of Future Technology, 2011.

[10] M. Lee, "The current state of CCTV regulations and its implications," *Korea Association for Telecommunications Policies*, vol. 18, no. 12, 2006.

[11] Y. Jo, "Efficient construction of an integrated control environment using an existing disaster briefing room," Regional Information, 2009.

[12] Korea Educational Center of Future Technology, *Business Outlook for Implementation Strategies of Next-Generation Video Surveillance and Intelligent Integrated Security Control Systems*, Korea Educational Center of Future Technology, 2011.

[13] I.-S. Lee and W. S. Yi, "Security requirements for network CCTV," *World Academy of Science, Engineering & Technology*, vol. 70, no. 47, p. 184, 2010.

[14] A. J. Lipton, C. H. Heartwell, N. Haering, and D. Madden, "Automated video protection, monitoring & detection," *IEEE Aerospace and Electronic Systems Magazine*, vol. 18, no. 5, pp. 3–18, 2003.

[15] L. Li, W. Huang, I. Y.-H. Gu, R. Luo, and Q. Tian, "An efficient sequential approach to tracking multiple objects through crowds for real-time intelligent CCTV systems," *IEEE Transactions on Systems, Man, and Cybernetics, Part B: Cybernetics*, vol. 38, no. 5, pp. 1254–1269, 2008.

[16] N. Buch, S. A. Velastin, and J. Orwell, "A review of computer vision techniques for the analysis of urban traffic," *IEEE Transactions on Intelligent Transportation Systems*, vol. 12, no. 3, pp. 920–939, 2011.

[17] T. D. Räty, "Survey on contemporary remote surveillance systems for public safety," *IEEE Transactions on Systems, Man and Cybernetics Part C: Applications and Reviews*, vol. 40, no. 5, pp. 493–515, 2010.

[18] KISA, *Global Information Security Industry Trend Survey Research*, Korea Internet Security Agency, 2013.

[19] KOTRA, International Business Product Information, Market Trends, 2013, http://tradedoctor.kotra.or.kr/.

[20] T. Seo, S. Lee, B. Bae, E. Yoon, and C. Kim, "An analysis of vulnerabilities and performance on the CCTV security monitoring and control," *Journal of Korea Multimedia Society*, vol. 15, no. 1, pp. 93–100, 2012.

[21] T. Seo, "A study on vulnerabilities of monitoring and control system based on IT convergence technology," in *Proceedings of the 6th International Conference on Multimedia Information Technology and Applications*, 2010.

[22] Trend Micro, *Blurring Boundaries: Trend Micro Security Predictions for 2014 and Beyond*, Trend Micro, 2013.