Chapter 22
Agent based Video Contents Identification and Data Mining Using Watermark based Filtering

HeungKyu Lee[1]

Abstract This chapter describes the agent based video contents identification scheme using watermark based filtering technique. To prevent a user from uploading illegal video contents into the WEB storages, two strategies are employed. First stage is the upload blocking of illegal contents including copyright ownership information as a watermark when a user tries to upload the illegal video content. Second stage is to monitor illegal video contents that are already uploaded. For this stage, the monitoring agent obtains video content link information, and then extracts the watermark from corresponding content using the Open API. For two stage video identification strategies, two types of watermark extraction schemes are employed. Gathered data obtained from agents is analyzed using data mining method, and reporting process is done. To show the effectiveness of the described system, some experimental evaluation and test are conducted.

22.1 Introduction

The multimedia digital data and representation service has emerged something valuable and applied and spread to the commercial system. With this wide spread, the security issue is also emerged because it can be copied easily without loss of quality and illegally distributed on the high speed network. To resolve this issue, multimedia contents protection technique to prohibit the unauthorized copying and redistribution of multimedia contents has researched. It includes the digital rights management (DRM), digital watermarking [8], and the feature (or signature) based fingerprinting [1][2][9]. The DRM is means to protect multimedia contents based on the cryptography. It has a weakness that decrypted multimedia data can be redistributed easily. Meanwhile, digital watermarking provides secure contents protection scheme because the watermark is included into the content itself by modifying the pixel in-

[1] Dept. of Electronics and Computer Engineering, Korea University, Seoul, Korea., E-Mail:hklee@ispl.korea.ac.kr

L. Cao (ed.), Data Mining and Multi-agent Integration, DOI: 10.1007/978-1-4419-0522-2_22,

tensity. Thus, it cannot be removed without destroying the value of the multimedia content. Therefore, embedding of unique user identification as a watermark into data can be used to identify illegal copies of multimedia contents. The identification number of a user buying content is embedded into the sold content. If an illegal copy is found, the malicious user's identification can be traced from the embedded identification. The feature based fingerprinting is means to find a highly similar content with a queried one in a stored feature database.

As a video content identification technique for protection of security and privacy, feature based fingerprinting technique is currently preferred choice. Recent works are done in [10][11][12]. However, the defect of the feature based fingerprinting technique is that the unique feature database of a large number of multimedia contents must be constructed [3]. In addition, feature based video fingerprinting system requires much time to extract video frame features and match them with feature vectors stored in a database. Thus, it is not sufficient to apply it to the practical and commercial products.

To cope with this issue, this chapter proposes the agent based multimedia contents identification scheme using watermark based filtering technique. Basically, watermark information embedded into multimedia data for enforcing copyrights must uniquely identify the data and must be difficult to remove, even after various media transformation process. To prevent a user from uploading video contents into the WEB server or the WEB hard disk, two strategies are employed. First stage is the upload blocking of illegal contents including copyright ownership using watermark by a contents blocking agent when a user uploads a video content. Second stage is to monitor and identify video contents that are already uploaded into the WEB storage. For this stage, a monitoring agent finds video contents that exists within a web server or in other locations, and extracts the watermark from them. To identify video contents that exist in other WEB server location, watermark extraction function using the Open API is provided.

22.2 Multagent Integration and Data Mining Concept

For agent based video contents identification, contents blocking agent and monitoring agent are used on a specific web site to provide data mining service for protection of security and privacy[18]. These agents can be located in every different web site [13][14]. The contents blocking agent only prohibits illegal contents by inspecting the presence of copyright ownership information using watermark extraction method. Meanwhile, the monitoring agent not only inspects the presence of copyright ownership information using more complex watermark extraction method, but also communicates with other site's monitoring agents to gather extra statistical information. This makes the multi-agent integration and data mining framework on distributed network environment [15][16][17]. This framework decreases unnecessary watermark extraction overloads that can be occurred repetitively by a monitoring agent.

Contents blocking agent is to prevent users from uploading copyrighted contents by simply extracting watermark information. Contents blocking agent has proactive role of preventing illegal contents distributions. This filtered some portion of illegal contents when users try to upload illegal contents. This decreases the server process overload of a monitoring agent to detect an illegal distribution of copyrighted contents using complex watermark extraction mode.

Monitoring agent extracts a watermark that represents copyright ownership information and traitor tracing information with complex extraction mode. This extracted information is stored in a database. Then, this information is queried to other monitoring agent located in other content providing server. If homogeneous content is stored on that server, the responded information is stored together to gather status information of the content with respect to the use of illegal distribution. This information provides statistical and relationship information that is not reliant on an existing database and has previously been discovered by monitoring agents of other specific sites without extra processing [18]. This decreases unnecessary watermark extraction overloads that can be occurred repetitively by a monitoring agent.

22.3 Watermark Embedding for Contents Identification

Two kinds of watermark information are embedded into the video contents as shown in Fig. 22.1. First watermark is embedded simultaneously when the contents are encoded for video on demand service. Meanwhile, second watermark is embedded when the demanded video is played. It requires real-time service. Thus, watermark pattern is generated at the display beginning time, and then represented on the graphics plane. The video frame is presented on the video plane of the STB device. To

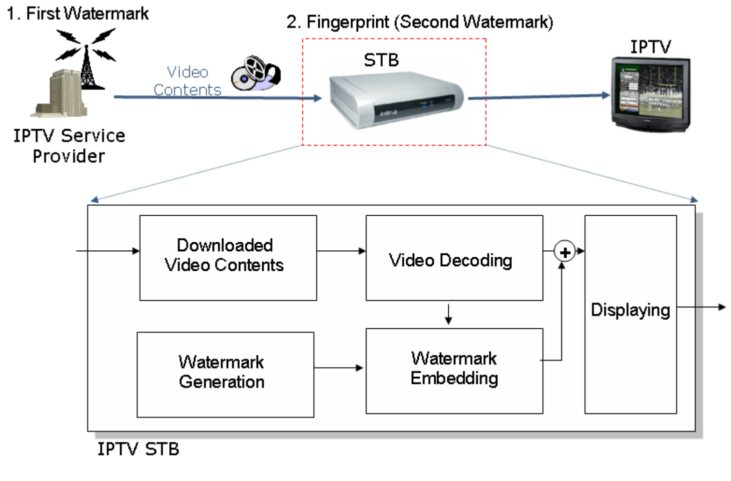


Fig. 22.1: Watermark embedding stage at the front-end and back-end system

reduce the computing time, the human visual system model is computed once per short time interval that we used 5 frame intervals experimentally. Finally, video and graphics plane are blended for displaying.

First watermark representing copyright ownership information is embedded at the back-end system. Two kinds of watermark signals are orthogonal between them because they have distinct secret key that is used for generation of random pseudo noise pattern. However, interference can be occurred between them if two signals are overlapped. Thus, first watermark is recursively embedded into specific time range positions TSi as shown in Fig. 22.2. The term, TSi represents the time range that first watermark can be embedded. It is assumed that an example video has 30 frames per second (FPS) as shown in Fig. 22.2. Second watermark representing buyer information is embedded at the front-end system that is set-top box device for IPTV. This watermark is called in fingerprints that are traitor tracing information. In the proposed system, the device ID and playing time information are embedded into specific time range positions TMi as shown in Fig. 22.3. The device ID can be associated with a user ID that was registered information in service application time. Thus, we can know his name and address if the embedded watermark is extracted. The playing time can be associated with a capturing time. From this information, we can know when and who captured the illegally uploaded video.

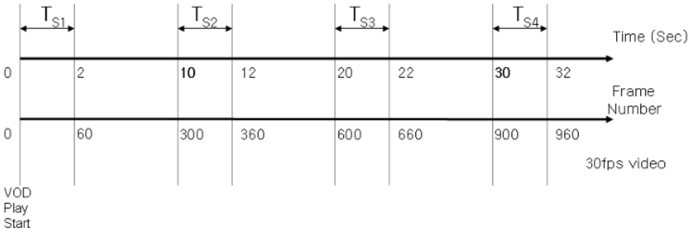


Fig. 22.2: First stage of watermark embedding: copyright ownership information is watermarked at the contents broadcasting side.

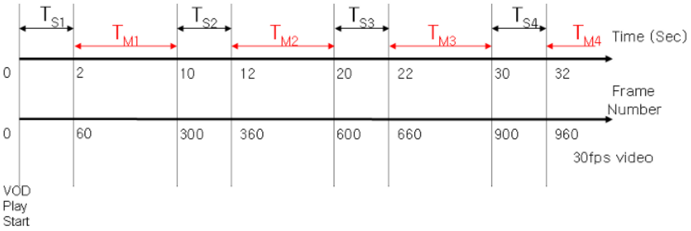


Fig. 22.3: Second stage of watermark embedding: User ID and playing time information is watermarked for traitor tracing at the STB device.

22.4 Agent based Content Blocking and Tracing

22.4.1 Contents Blocking Agent

The role of content blocking agent is to prohibit an illegal content from uploading into a Web server when a user tries to upload it. The one of the issues in video contents identification is fast computation time. Especially, file upload blocking technique requires nearly real-time computing speed because file upload speed is very fast. So, watermark extraction speed must be highly fast. To cope with this, the content blocking agent uses simple watermark extraction technique as shown in Fig. 22.4. Under consumption that the content is not attacked or only scale down attack is done, watermark extraction is performed. If the copyright ownership information embedded in Fig. 22.2 is extracted, the warning message is displayed on the user's screen and then uploading is prohibited. Generally, scaling down attack is frequently occurred one in case of a video intentionally or unintentionally. If we use a HD (High-Definition) video in watermark embedding time as shown in Fig. 22.1, we can predict that the content is transformed from a HD resolution to a SD one. So, direct geometrical recover is done, and then extracts a watermark. In addition, compression and digital filtering attacks do not change geometric parameters. Direct watermark extraction without considering attack and watermark extraction considering scaling down prediction are very useful strategy. Actually, 50% of illegal video contents can be prohibited in uploading time.

22.4.2 Monitoring Agent

The role of the monitoring agent is to examine already uploaded video contents once again by detailed watermark extraction method. In addition, it gather the illegal contents distribution information from other web site's monitoring agents.

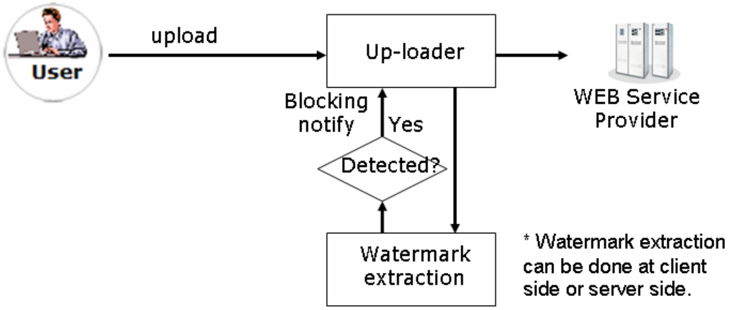


Fig. 22.4: Watermark based file upload blocking scheme using an agent. Watermark extraction can be done at client side or server side by the agent.

For traditional content searching, the web robot is generally used. It is often called as web wanderers, web crawlers, or web spiders. The web robot is a software based agent that automatically traverses the web's hypertext structure by retrieving a document and recursively all referenced documents. However, traversing the Internet and collecting contents requires tremendous time and storage. In addition, it can give the network and server overload. To reduce these faults, some effective method is proposed in [4]. For example, Digimarc's MarcSpider [5] is the traditional web robot based image tracking system that is the first trial to detect watermarked content on the web. MarcSpider uses hundreds of individual web spiders that look through the web to search for images that is watermarked one. However, it can not trace illegal distributor but prove only the copyright ownership information of that image. In addition, the traditional content searching method based on the web robot has still network and server overload even if the optimal searching is developed. It is a time consuming process. To resolve this issue, the monitoring agent provides the open API functions as shown in Fig. 22.5. The content search and watermark extraction functions are provided between the monitoring agents. For doing this, video content management database is constructed. The location of a video and service menu name is stored in a database. Thus, the monitoring agent at the site A requests contents link information to the one at the site B using the Open API function. Then the monitoring agent at the site A request the watermark extraction result of a specific content URL using a secret key to the one at the site B using the Open API function.

The contents link information is also stored in a database, and then its information is updated by periods. This content link information table includes the le-

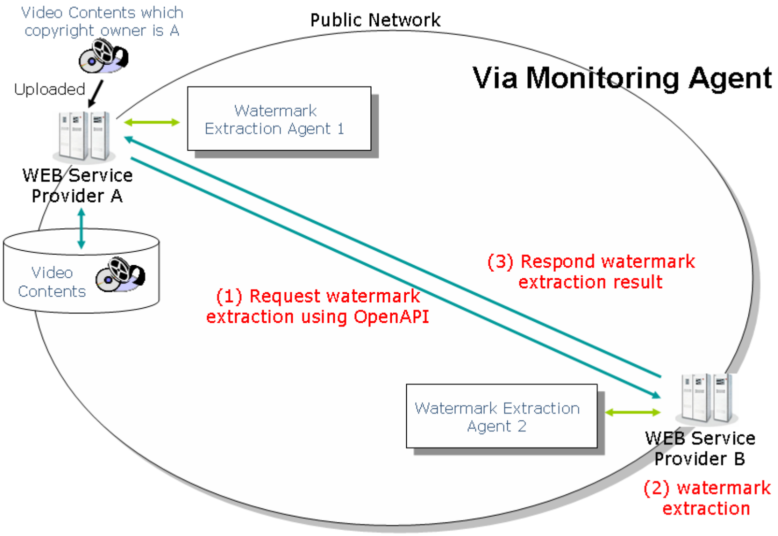

Video Contents which copyright owner is A
Public Network
Via Monitoring Agent
Uploaded
Watermark Extraction Agent 1
WEB Service Provider A
Video Contents
(3) Respond watermark extraction result
(1) Request watermark extraction using OpenAPI
Watermark Extraction Agent 2
WEB Service Provider B
(2) watermark extraction

Fig. 22.5: Watermark based monitoring and identification scheme using an agent. Video contents can be identified irrespective of their location by using watermark extraction Open API function.

gal/illegal type field. This field is updated after watermark extraction. Thus, the monitoring agent has only to extract a watermark from a newly updated content. This process does not require network usage and burden for uploading and downloading contents. So, it provides the very practical content tracing function. The response of the Open API function is returned with the requested information. The monitoring agent saves only the updated link information by comparing it with the content link database. Then, the updated contents are requested for watermark extraction. This procedure can be repeated by periods.

22.4.3 Data Mining and Reporting Process

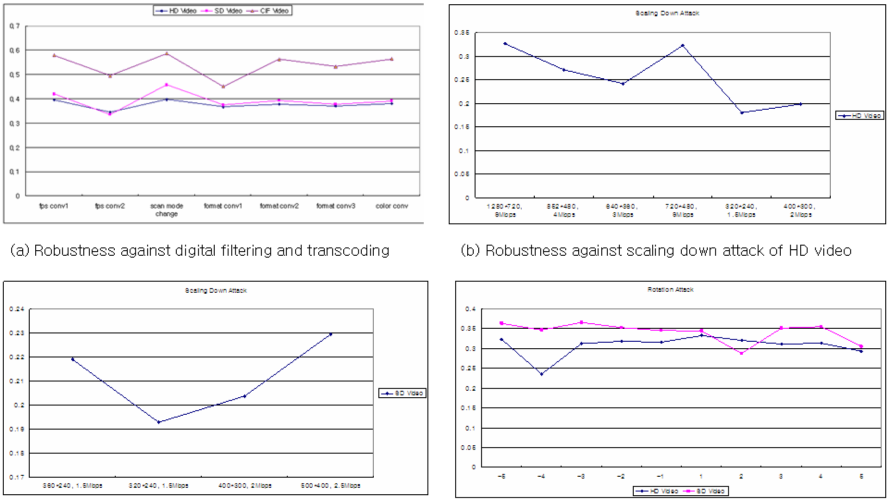
The watermark is extracted by the content blocking agent and the monitoring agent. These two agents are located in the specific site A. They have their own database to record a watermark extraction result and its behavior. The content blocking agent has a record that is content blocking result after watermark extraction. This information is only used as reference information because the illegal content is not uploaded. However, we can know how many contents the specific person tried to upload from the analysis. The monitoring agent has records that are copyright ownership information and its traitor tracing information of contents. This information can be directly provided to the content providers. In addition, it is notified to the specific site's administrator in order to delete the illegal content.

The gathered information by the content blocking agent and the monitoring agent is data mined to obtain the statistics and valuable information with respect to the uploaded contents, specific site, and illegal users. The result is represented by summary table and multiple level-of-abstraction rules to associate it with a meta content database [6][7]. This mining result exists in every web site. Thus, the copyright protection center such as governmental organization can gather the mined results in each web site for second data mining. After first mining phase of the process is finished, the system has produced the final set of illegal contents statistics. The final sets can be obtained from the web sites. Then we proceed to the post-processing step for data enrichment. Data originating from different parts of the websites are gathered and integrated with the data mining results. The goal of data enrichment is to take as input the illegal contents statistics, and correlate them with all the relevant fields of information. The enriched statistics information that was produced during the data enrichment phase can then be analyzed. Finally, a series of reports summarizes the results of the previous data analysis phases. According to the first watermark information, they can analyze which site or service has a defect.

22.5 Experimental Evaluations

The proposed method's prototype system has developed in order to detect and trace video contents in Windows XP environment. The database is constructed using SQL server, and the Aparch web server is used. The system use ODBC to manage the content link information and blocking information. The prototype system is tested on the designated web sites, which has watermarked video contents. In addition, illegal contents are tried to upload video contents. From the test results, we obtained 100% of retrieval rate. This retrieval rate is actually associated with the watermark extraction accuracy. The employed watermark extractor is developed against compression, digital filtering, scaling, and rotation attacks as shown in Fig. 22.6. Figure 11, (a) presents a robustness against frame rate change (30− >25, 30− >15), scanning mode change from interlaced to progressive, video format change from MPEG-2 to H.264/AVC, Flash, MPEG-4, and color conversion from color to gray. Figure 11, (b) presents a robustness against scaling down attack of a HD video from 1920*1080 resolution to 1280*720, 852*480, 640*360, 720*480, 320*240, and 400*300 one. Figure 11, (c) presents a robustness against scaling down attack of a SD video from 720*480 resolution to 360*240, 320*240, 400*300, and 500*400 one. Figure 11, (d) presents a robustness against rotation attack ranged between -5' and 5'.

Under the assumption of the content blocking agent, compressed and digital filtered watermarked videos are prohibited from uploading. In addition, known scaling attacked video is blocked. However, the watermark failure is occurred with respect to the compositely attacked videos. The content blocking agent is downloaded into the user's PC, and then is installed. The watermark extraction processing is done



(a) Robustness against digital filtering and transcoding

(b) Robustness against scaling down attack of HD video

(c) Robustness against scaling down attack of SD video

(d) Robustness against rotation attack

Fig. 22.6: The watermark extraction robustness against attacks

on user's machine. Thus, it does not give the processing overload to the web server. Meanwhile, 50% of CPU resource is required on the user's machine. The monitoring agent is installed on a PC server that is connected via the Internet with a web server because the watermark extraction requires high CPU and memory resource. It has access privilege of contents located in the web server. The monitoring agent obtains content link information using the Open API and can request watermark extraction. Meanwhile, the monitoring agent extracts a watermark from a specific content that is requested from the monitoring agent of the other site.

Fig. 22.7 represents comparison between agent-mining based and non-agent-mining based video content identification. Total 1,000 numbers of copyrighted video contents are used for experimental evaluations of site A and site B where 15% of redundant videos are included. In non-agent based video content identification, watermark detection rate was 95% and CPU overload was 80%. But, in agent based video content identification, watermark detection rate was same in non-agent based one while CPU overload due to watermark extraction was distributed. In addition, CPU overload is decreased into average 32.5% by removing unnecessary watermark extraction with communicating between the monitoring agents.

22.6 Conclusion

In this chapter, the agent based video contents identification scheme using watermark based filtering technique is described. To prevent a user from uploading illegal video contents into the WEB storages, watermark based filtering technique based on the agents are employed. First stage is the upload blocking of illegal contents including copyright ownership by extracting a watermark when a user try to upload illegal

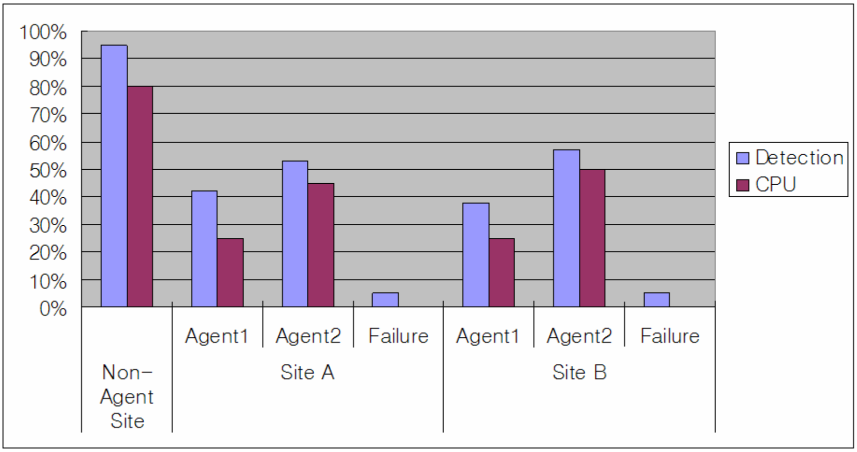


Fig. 22.7: The watermark extraction robustness against attacks

video content. Second stage is to monitor video contents that are already uploaded. For this stage, the monitoring agent obtains video content link information that exists within a web server, and then extracts the watermark from them using Open API. Gathered information obtained from agents is analyzed using data mining method, and reporting process is done.

References

1. J. Haitsma and T. Kalker, ”A highly robust audio fingerprinting system,” in Proc. Int. Conf. Music Information Retrieval, 2002.
2. P. Cano, E. Batlle, T. Kalker, and J. Haitsma, ”A review of algorithms for audio fingerprinting ,” in Proc. IEEE Workshop Multimedia Signal Processing, pp. 169-173, 2002.
3. B. Chor, A. Fiat, M. Naor, and B. Pinkas, ”Tracing Traitors,” IEEE Trans. Inf. Theory, Vol.46, pp.893-910, May 200
4. M. Koster, ”WWW Robots, Wanderers and Spiders,” URL:http://www.robotstxt.org/wc/robots.html
5. Digimarc Corporation, http://www.digimarc.com
6. J. Han, Y. Cai, and N. Cercone, ”Data-Driven Discovery of Quantitative Rules in Relational Databases,” IEEE Trans. on Knowledge and Data Eng., vol. 5, pp.29-40, 1993.
7. C. Bohm, S. Berchtold, and D. Keim, ”Searching in high-dimensional spaces: Index structures for improving the performance of multimedia databases,” ACM Comput. Surv. Vol. 33, no. 3, pp.322-373, 2001.
8. I. J. Cox, J. Killian, T. Leighton, and T. Shamoon, ”Secure spread spectrum watermarking for multimedia,” Tech. Rep. 95-10, NEC Research Institute, 1995.
9. J. Oostveen, T. Kalker, and J. Haitsma, ”Feature extraction and a database strategy for video fingerprinting,” in Proc. Int. Conf. Recent Adv. Vis. Inf. Syst., 2002, pp. 117-128.
10. Changick Kim and Bhaskaran Vasudev, ”Spatiotemporal Sequence Matching for Efficient Video Copy Detection,” IEEE Trans. On Circuits and Systems for Video Technology, Vol.15, NO.1, pp.127-132, Jan. 2005.
11. Li Chen, and F.W.M. Stentiford, ”Video sequence matching based on temporal ordinal measurement,” Pattern Recognition Letters, Vol.29, pp.1824-1831, 2008.
12. Sunil Lee and Chang D. Yoo, ”Robust Video Fingerprinting for Content-Based Video Identification,” IEEE Trans. On Circuits and Systems for Video Technology, Vol.18, No.7, pp.983-988, July 2008.
13. Androutsellis-Theotokis, S. and Spinellis, D.: A Survey of Peer-to-Peer Content Distribution Technologies, ACM Computing Surveys, Vol. 36, No. 4 (2004) 335-371.
14. V. Gorodetskiy, O. Karsaev, V. Samoilov, S. Serebryakov. P2P Agent Platform: Implementation and Testing. The AAMAS Sixth International Workshop on Agents and Peer-to-Peer Computing (AP2PC 2007), Honolulu, 2007 pp. 21-32.
15. V. Gorodetskiy, O. Karsaev, V. Samoilov, S. Serebryakov. Multi-Agent Peer-to-Peer Intrusion Detection. MMM-ACNS-2007. In series ”Communication in Computer And Information Systems”, volume 1, Springer 2007, pp. 260-271.
16. C. Giannella, R. Bhargava, H. Kargupta, M. Klusch, J.C. Da Silva (2005): Distributed Data Mining and Agents. Journal of Engineering Applications of Artifical Intelligence, 18(4), Elsevier Science
17. H Kargupta, B Park, D Hershberger, E Johnson, ”Collective data mining: A new perspective toward distributed data mining,” Advances in Distributed and Parallel Knowledge Discovery, 1999.
18. Longbing Cao, Chao Luo, Chengqi Zhang. Agent-Mining Interaction: An Emerging Area, AIS-ADM07, LNAI 4476, 60-73, Springer, 2007.