



Annual ADFSL Conference on Digital Forensics, Security and Law

2011
Proceedings

May 25th, 3:45 PM

Development of A Distributed Print-Out Monitoring System for Efficient Forensic Investigation


Satoshi Kai

Hitachi, Ltd., Yokohama Research Laboratory, Graduate School of Informatics, Kyoto University

Tetsutaro Uehara

Associate Professor, Academic Center for Computing and Media Studies, Kyoto University

Follow this and additional works at: <https://commons.erau.edu/adfsl>

 Part of the [Computer Engineering Commons](#), [Computer Law Commons](#), [Electrical and Computer Engineering Commons](#), [Forensic Science and Technology Commons](#), and the [Information Security Commons](#)

Scholarly Commons Citation

Kai, Satoshi and Uehara, Tetsutaro, "Development of A Distributed Print-Out Monitoring System for Efficient Forensic Investigation" (2011). *Annual ADFSL Conference on Digital Forensics, Security and Law*. 2.

<https://commons.erau.edu/adfsl/2011/wednesday/2>

This Peer Reviewed Paper is brought to you for free and open access by the Conferences at Scholarly Commons. It has been accepted for inclusion in Annual ADFSL Conference on Digital Forensics, Security and Law by an authorized administrator of Scholarly Commons. For more information, please contact commons@erau.edu.

EMBRY-RIDDLE
Aeronautical University™
SCHOLARLY COMMONS

(c)ADFSL



DEVELOPMENT OF A DISTRIBUTED PRINT-OUT MONITORING SYSTEM FOR EFFICIENT FORENSIC INVESTIGATION

Satoshi Kai

Hitachi, Ltd., Yokohama Research Laboratory
292 Yoshida, Totsuka-ku, Yokohama, Kanagawa 244-0817, Japan
Graduate School of Informatics, Kyoto University
Yoshida-Honmachi, Sakyo-ku, Kyoto 606-8501, Japan

Tetsutaro Uehara

Associate Professor
Academic Center for Computing and Media Studies, Kyoto University

ABSTRACT

If information leakage occurs, an investigator is instructed to specify what documents were leaked and who leaked them. In the present work, a distributed print-out monitoring system—which consists of a virtual printer driver and print-out policy/log management servers—was developed. For easily matching the discovered (i.e., leaked) paper document with the print-out log, the virtual printer driver acquires full-text of printed-out documents by DDI hooking technique to check the content, transforms a spool file to a picture file and creates both a thumbnail and text log for forensic investigation afterwards. The log size is as only about 0.04 times bigger than that for printed-out electronic documents, so the storage size needed for the thumbnail and text log is also small.

Keywords: Information leakage, Print-out, Digital forensics, Log, Virtual printer driver

1. INTRODUCTION

Information leakage is one of the most serious incidents facing a company or an organization. Many leakage incidents happen in the form of documents. As for documents created in an office, it was found that 93% are in electronic form and 7% are in paper form (Kevin 2000 [1]). However, 72.6% of leakage routes are known to be via paper medium (JNSA 2010 [2]). In other words, although paper documents make up a smaller percentage of the total amount of documents, they are the main cause of information leakage. Since information-communication technology (ICT) is becoming ever more common in all styles of working, these paper documents are considered to be those created in electronic form first and then printed-out in paper form. Accordingly, the security of such print-out matter is an important factor in preventing and detecting information leakage.

Once information leakage occurs, the company or organization starts incident response using digital forensics. According to Takahashi 2008 [3], this response is composed of following steps.

1. Detection
2. Initial response
3. Investigation
4. Disclosures
5. Restraint and recovery
6. Post incident

From start to finish of this incident response, digital forensics is used to determine leakage facts such as what documents were leaked and who leaked them.

In the present work, a print-out monitoring system is in place that prevents illegal print-out according to the content under usual working circumstances as well as supports digital forensics when information leakage occurs. Moreover, this system is easy to install on existing PCs and requires less storage size to accumulate the print-out logs.

2. DIGITAL FORENSIC SCENARIO CONCERNING INFORMATION LEAKAGE

2-1. Supposed information-leakage incident

Information-leakage incidents differ from one to another in terms of situation, impact, and so on. To clarify situations and motivation concerning digital forensic, an incident such as that shown in Fig. 1 is presented in this paper. This scenario is taken and modified from a report issued by the Tokyo Metropolitan Police Department in 2010 [4].

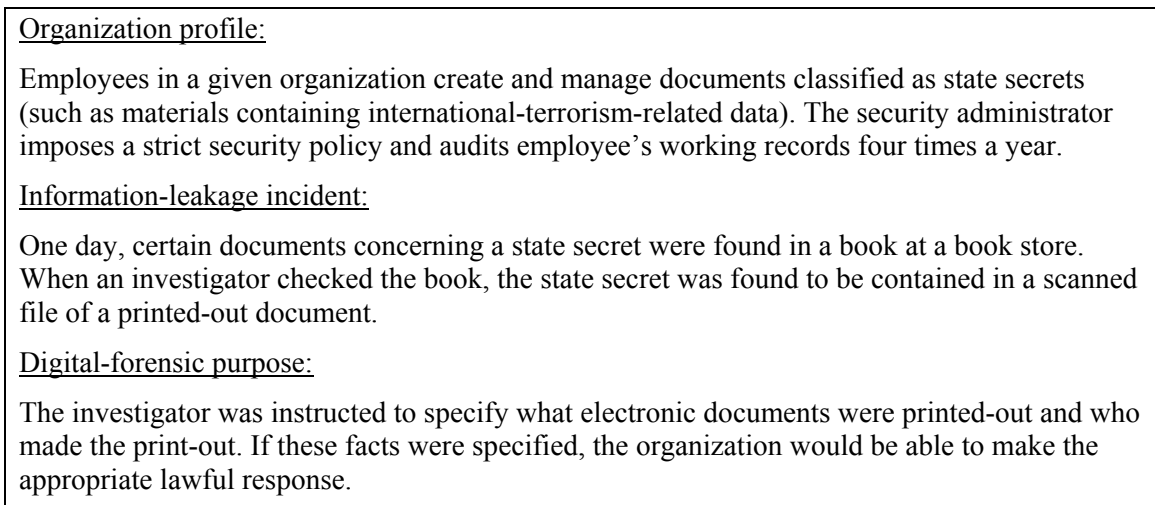


Fig. 1: Supposed organization and information-leakage incident

2-2. Supposed document-management model

The organization must manage the documents properly and prevent information leakage. Typical document-management models are classified as a central-management model or a distributed model.

2-2-1. Central-document-management model

The central-document-management model (see Fig. 2) is one of client-server models. Clients are "dumb terminals," which can only handle "KVM" (keyboard, video, and mouse) operations, i.e., not storage. The servers are file servers and document-management servers. All documents created by users are stored only on the server side, and any paper documents are printed out on the shared printer. Any printed-out documents are therefore almost identical to the original one on the server side (see broken arrow in Fig. 2).

If the information leakage mentioned in section 2-1 occurs, the investigator must collect and search both the print-out logs at the shared printer and the documents on the server side (see unbroken arrow in Fig. 2). These days, search engines are used widely on the server side, so they are useful for supporting digital forensics.

The central-management model is ideal in regard to digital forensics because the investigator only has to collect and search documents on the server side.

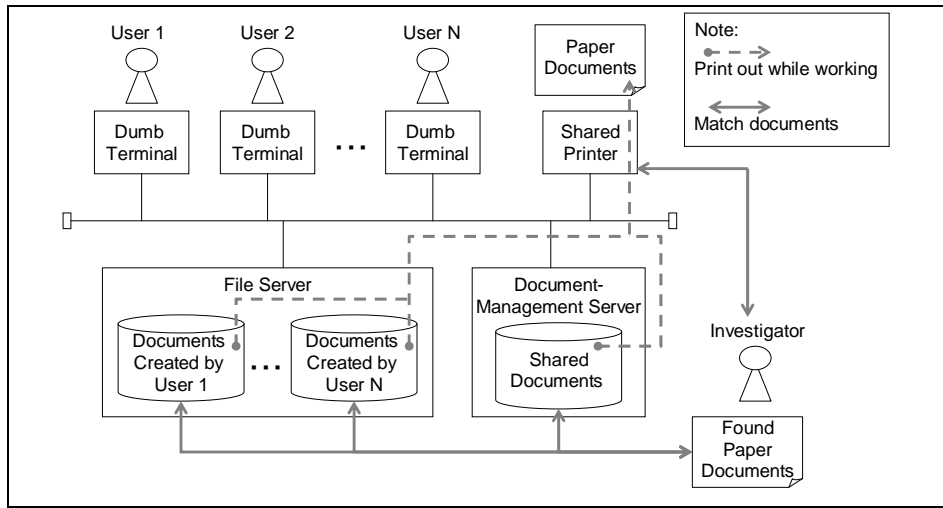


Fig. 2: Central-document-management model

2-2-2. Distributed-document-management model

The distributed-document-management model (see Fig. 3) is a client-server model in which the clients are PCs that can handle storage. The servers are the same as those in the central-document-management model. The documents created by a user are stored on both the server side and the client side. Any printed-out documents are thus almost identical to those on both the server side and the client side (see broken arrow in Fig. 3).

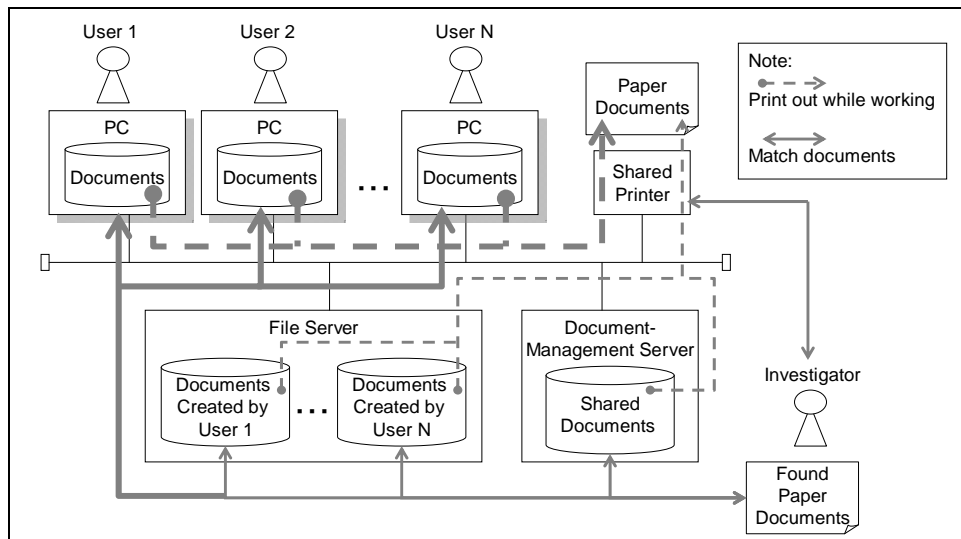


Fig. 3: Distributed-document-management model

If the information leakage mentioned in section 2-1 occurs, the investigator must collect and search the print-out logs at the shared printer, the documents on the server side, and the documents on the client side (see solid unbroken arrow in Fig. 3). In particular, the documents on the client side are sometimes hard to investigate because many more PCs may exist on the client side than on the server side and because not only complete versions of documents but also incomplete manuscripts in poor order exist. The present study focused on the distributed-document-management model (Fig. 3) and especially addresses collecting and searching the printed-out documents on the client side.

By the way, it may be considered that the documents are transported electronically to an off-site location (e.g., via flash drive or email) and then printed-out. In that case, the documents can be protected by a conventional digital rights management (DRM) function [5][6]. By using the DRM, print-out can be controlled from the central DRM server. But this DRM is only useful for delivering the documents, not creating and modifying. So DRM is out of scope of the present study.

2-3. Digital-forensic techniques for print outs

Digital forensics includes many investigation procedures. To specify what electronic documents were printed out and who did the printing out, the following procedure, shown schematically in Fig. 4 as four steps, is used for digital-forensic investigations on Windows PCs. Note that Unix PCs or Mac PCs can also be investigated using almost the same or alternative steps. However, Windows PCs are used widely, so this study addresses information leakage with Windows PCs.

Step1: Check the registry key, such as “HKEY_LOCAL_MACHINE/SYSTEM/CurrentControlSet /Control/Print/Printers.” If no printer driver is installed, the PC is judged to be not used for print outs; that is, it is not suspected of information leakage.

Step2: Check the event log, such as event ID10, ID540, and ID560 (Microsoft’s Log Audit Guide 2007 [7]). If no print-out log is recorded, the PC is judged to be not used for print outs; that is, it is not suspected of information leakage.

Step3: Check the spooler located at “C:/WINDOWS/system32/spool/PRINTERS”. If any residual spool files are left, the investigator can match the printed-out image with the found paper documents.

Step4: Check the documents listed in the print-out log so that the investigator can match the documents with the discovered paper documents and specify when and where the document was printed out and who printed it out.

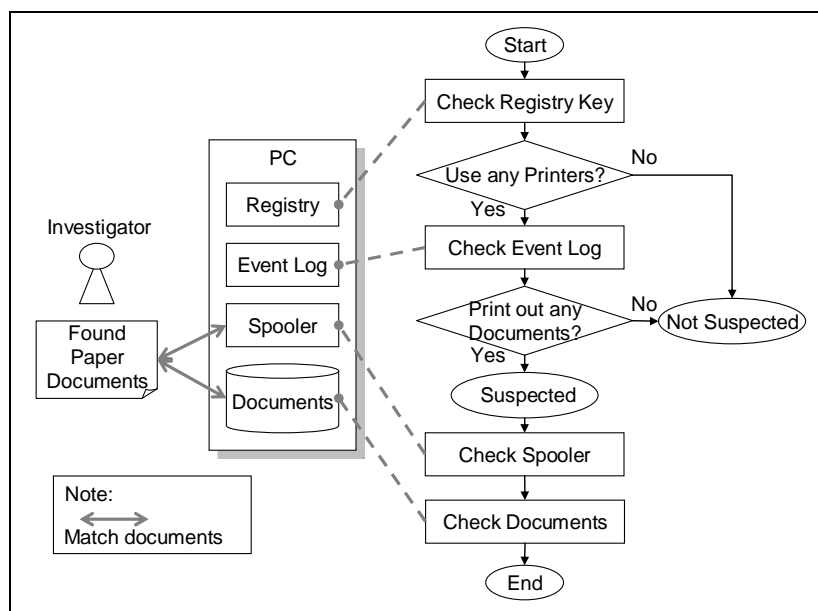


Fig. 4: Digital forensic procedure for identifying printed-out documents with found paper documents.

2-4. Problems

The above-mentioned digital-forensic procedure for investigating print outs is sometimes useful, but it suffers the following residual problems.

Problems 1: Uncertainty regarding what documents were printed out.

The Windows event log records “print job name”, which depends on each print-out application and often includes only the file name, not the file path. The investigator thus cannot always match what documents were printed-out with the discovered paper document, even if the investigator knows the print job name. Moreover, spool files are deleted after succeeding print outs and overwritten one by one. Recovering the spool files is therefore difficult.

Problems 2: It takes a lot of time to collect and confirm the registry, event log, and spool file.

The number of client PCs exceeds that of servers, and the PCs are distributed in a variety of places. Moreover, access to the registry, event log, and spool file needs an administrator privilege for each PC. Consequently, acquiring the registry, event log and spool file data takes more time to collect and confirm.

3. DESIGN OF THE DISTRIBUTED PRINT-OUT MONITORING SYSTEM

To solve the problems described in section 2-4, a distributed print-out monitoring system was designed and constructed.

3-1. Operational model

When an employee needs to print out a document, he (or she) must install the printer driver of the shared printer. The printer driver is often provided by the print server. Even if PCs are distributed in a variety of places, the printer driver can be managed by the print server. The monitoring system was designed with a focus on the printer driver. Moreover, the supposed organization has a strict security policy, so the monitoring system is also equipped with a print-out control function that benefits both users and security administrators. The design of the operational model is shown schematically in Fig. 5.

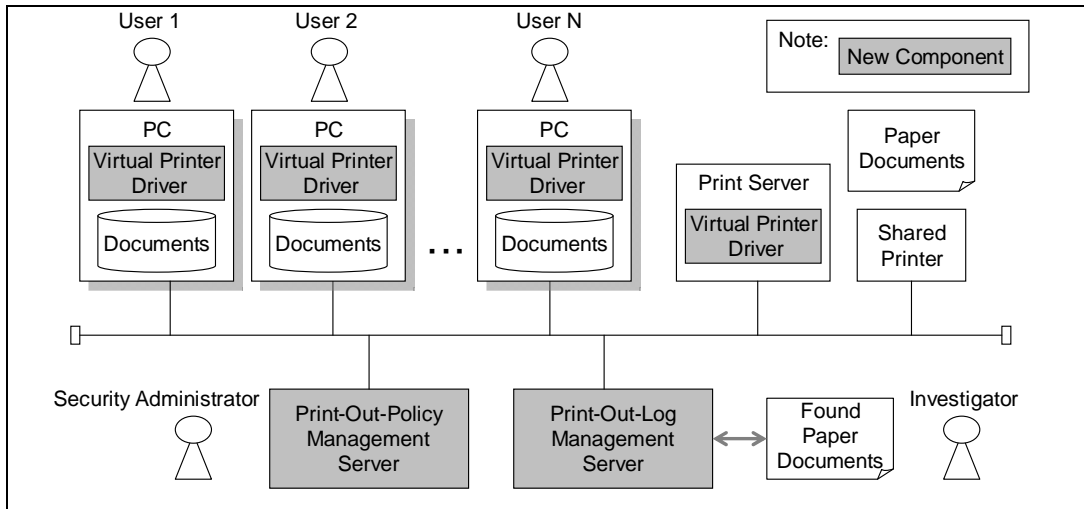


Fig. 5: Operational model of distributed print-out monitoring system

Users perform their business as following:

- (1) Users install a virtual printer driver from the print server on each PC.
- (2) Connected with the print-out-policy management server, the virtual printer driver checks the print-out content and controls the print jobs on each PC.
- (3) The virtual printer driver acquires the print-out logs and sends them to the print-out-log management server.

If an information leakage occurs:

- (4) The investigator searches the print-out logs to match a log entry with the leaked paper document.

3-2. Print-out logs

The print-out log is the key to match the log with the found paper documents. The print-out log consists of three items: (1) a spool file itself, (2) a picture file (transformed from (1)), and (3) a spool file acquired as text. These items are compared in Table 1.

The spool file, item (1), itself is sure to match the leaked paper document, but it needs to be re-printed out. The picture file, item (2), is easy to match with the leaked paper document without having to be re-printed out. However, its file size is prone to be big, and optical character recognition (OCR) is not always accurate in the case of text search. The text file, item (3), is easy to search, and the file size tends to be small. However, figures, pictures, and document layout are dropped from item (3).

To find interesting logs in a large amount of print-out logs, item (3) (text) is useful. On the other hand, to match the leaked document, (1) (spool file) or (2) (picture file) is useful. Accordingly, the print-out log was selected to be hybrid, both a picture file and text. Moreover, the picture file was selected to be thumbnails of all the pages of the printed-out document.

Table 1: Comparison of print-out-log items (1), (2), and (3)

Items	(1) Spool file	(2) Picture file	(3) Text
Examples	RAW, EMF, XPS, PS	JPG, PNG etc.	TXT
Match with leaked paper document	Easy	Easy	Not always easy (figures, pictures, and layout are dropped)
Need to re-print-out	Yes	No	No
Log file size	Prone to be big	Prone to be big	Tends to be small
Find an interesting log	Need to find by eye	OCR can be used to extract text (but prone to be incorrect)	Easy to text search.

The print-out-log format and its supposed size are listed in Table 2.

Table 2: Print-out log format

Items	Description	Supposed size
Date	Year, month, day, hour, minutes, seconds	14 bytes
User	Username	≤20 bytes
Printer	Printer name	≤32 bytes
Print job name	Print-job name (depends on print-out application)	≤255 bytes (possibly)
Page number	Number of printed-out pages	≤4 bytes
Content	Thumbnail	Thumbnails of each page
	Text	Full text of all pages

3-3. Print-out control

The print job is a key to control printing out documents. However, the print job itself is hard to check according to its content. Accordingly, it was decided to extract text information stored on the virtual printer driver, to check its content of text information, and to allow or prohibit the print job to send to the shared printer. Extracting text information from the text print-out log is described in section 3-2.

Checking text typically follows two strategies: (1) index search and (2) GREP search. These strategies are compared in Table 3. Index search is fast but not accurate; that is, precision and recall rate (Ricardo et al. 1999 [8]) is not always 100%. In detail, precision rate means the fraction of retrieved documents that are relevant to the search, and recall rate means the fraction of the documents that are relevant to the query that are successfully retrieved. In contrast GREP search is accurate; that is, recall rate is always 100%, but speed is low. From the viewpoint of checking text, precision below 100% is allowed but recall rate below 100% is never allowed because of the possibility of missing the interesting print-out logs. Strategy (2) (GREP search) was thus chosen for checking text.

Table 3: Comparison of strategies for checking text

Strategy	(1) Index search	(2) GREP search
Search speed	Fast	Slow
Spare resource before search	Indexing time and storage space for index files are needed.	Spare time and storage are not needed.
Precision	$\leq 100\%$	$\leq 100\%$
Recall	$\leq 100\%$	Always equals 100%

Examples of the GREP search keywords are listed in Table 4. These keywords are set by the security administrator on the print-out policy-management server. Alternatively, the investigator may set them on print-out-log management server when performing GREP search of the print-out logs.

Table 4: Examples of keywords

Category	Keywords sample
Confidential	“Confidential”, “Do not print”, “Internal use only”, etc.
Customer	Customer name (depends on each organization or business), credit-card numbers (often expressed by regular expression), etc.

3-4. Digital forensic use

When the investigator uses the distributed print-out monitoring system (Fig. 5), the following procedure is followed step by step.

Step1: Extract characteristic keywords in the leaked paper document

Step2: Perform GREP search for the print-out logs containing those keywords

Step3: Check the thumbnail pictures matched by the keywords, then match the thumbnails with the leaked paper documents.

Step4: Determine when the document was printed out (according to the print-out logs) and who did the printing.

By following this procedure, even if the client PCs are distributed widely, the investigator can collect print-out logs and search them accurately and efficiently. This procedure thus solves the problems stated in section 2-4.

4. IMPLEMENTATION OF VIRTUAL PRINTER DRIVER

4-1. Basic function of printer driver

A printer driver is a program (called by a print-out application) that sends a print job to a printer (Microsoft Developer Network 2010 [9]). The process followed by the printer driver is typically classified as two processes: layout arrangement and character output. Layout arrangement determines how many pages are needed and where to arrange characters and figures, etc. in the pages. Character output determines font, size, color, and decoration of the characters. Especially, the characters included in an electronic document are used as the input of the character-output process (see Fig. 6). For example, “a” is expressed by the character code “U+0061” in an electronic document. The character-output process transforms the code “U+0061” to the shape of “a”.

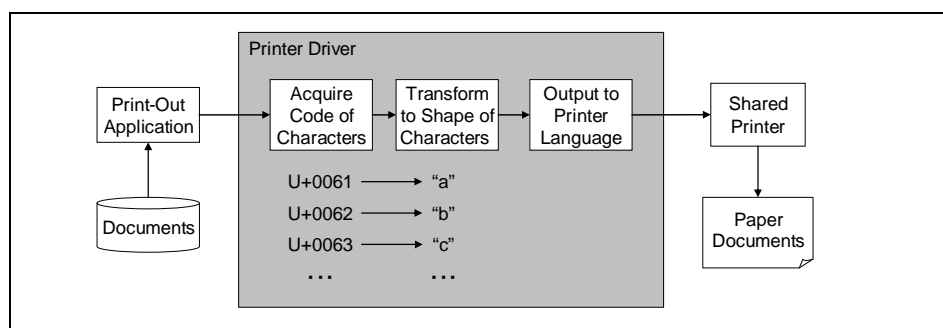


Fig. 6: Outline of character-output processing

4-2. Virtual printer driver

The virtual printer driver is a key component of the distributed print-out monitoring system. It is generally called a print-out application and sends a print job as a bitmap file, which can be printed out by a real printer driver of any kind. The architecture of the virtual printer driver is shown in Fig. 7.

When a character code is acquired, a DDI (device-driver-interface) hooking technique (Microsoft Developer Network 2010 [10]) modifies the acquisition process and transforms the characters into Unicode character code. All the characters are connected to be full-text and the full-text is then checked by the GREP search. If any NG keywords are included, the print job is deleted and the print out is stopped. If no NG keywords are included, both a text log and a thumbnail log are created and sent to the print-out-log management server.

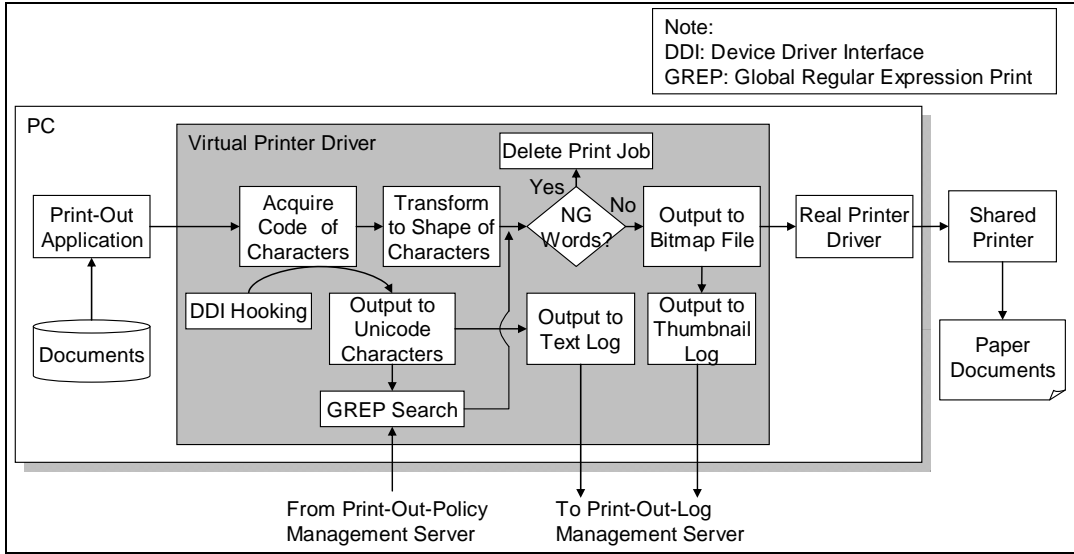


Fig. 7: Architecture of virtual printer driver

4-3. DDI hooking

The virtual printer driver was implemented on Windows XP SP3. The pseudo-code is shown in Fig. 8. The document print-out process begins with a DrvStartDoc call and ends with a DrvEndDoc call. For each physical page, the page-print-out process begins with a DrvStartPage call and ends with a DrvSendPage call. Between the DrvStartPage call and the DrvSendPage call, rendering operations and DrvTextOut are called as needed.

DDI hooking is provided by the Windows OS. By using that, the developer can refer or modify many kinds of the print-out control information. By hooking the DrvTextOut call, all characters code can be acquired. The hooking process is shown schematically in Fig. 8.

Original Code	DDI Hooking Code Added
DrvStartDoc ←	• Get Policy from Print-Out-Policy Management Server.
For each physical page {	
DrvStartPage {	
Rendering operations;	
DrvTextOut; ←	• Acquire code of characters, transform it to Unicode character code and make up full text.
}	
DrvSendPage ←	• Acquire thumbnail picture of each page.
}	
DrvEndDoc ←	• Check the full-text by GREP search. If includes NG words then delete print job. Send text log and thumbnail log to Print-Out Log-Management Server

Fig. 8: Pseudo-code with DDI hooking process added

An example of a print-out log is shown in Fig. 9. The thumbnail picture is set as a JPEG file with a size of 181 × 256 pixels because the thumbnail picture included in the XPS file has the same specification (Microsoft 2010 [11]).

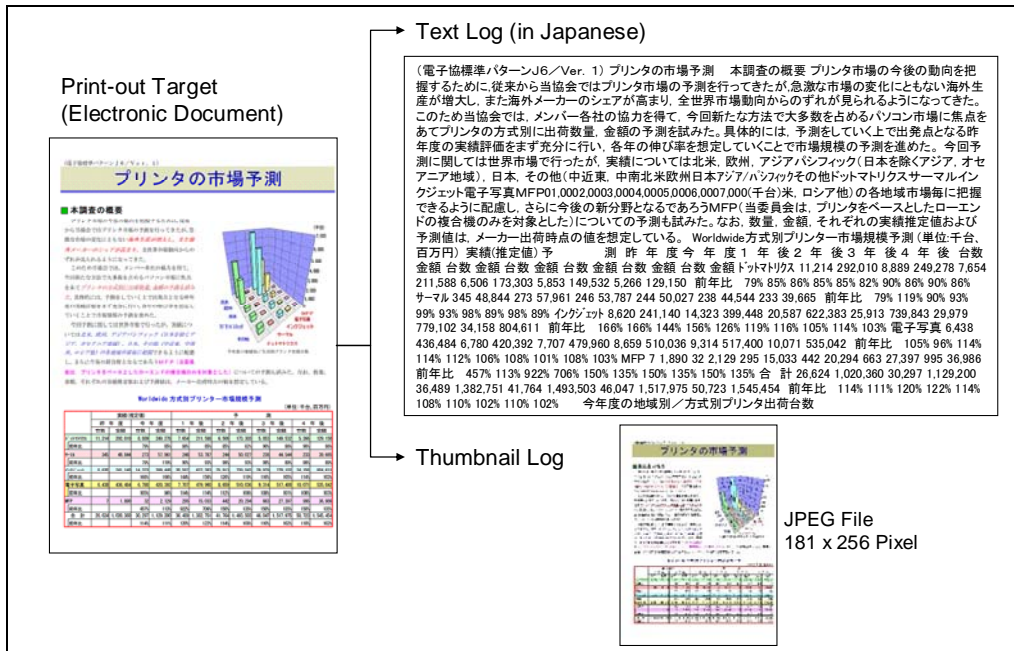


Fig. 9: Example print-out logs

4-4. Searching Japanese text

English and Japanese differ in that English sentences have blanks between words to distinguish each word and that Japanese does not separate words with blanks. Chinese and Korean have the same characteristics as Japanese. So a GREP search is prone to be slower in the cases of Japanese, Chinese, and Korean. To distinguish every word, morphological-analysis tools [12][13][14] are known to be useful. Using both the GREP search and morphological-analysis tools is one way to search Japanese text.

By using the morphological-analysis tools, the full-text is divided into each word. Especially the noun words tend to be divided exactly. Many keywords are usually noun words, so the tools influence little on search leakage.

5. EVALUATION OF PRINT-OUT LOG SIZE

The print-out log is better if its size is smaller. The following evaluation addresses the size of the print-put log.

5-1. Precondition

Print-out log size depends on the target electronic documents. To standardize the evaluation, standard-test-patterns for printers were used (JEITA 2003 [15]). In Fig. 9, one of the test patterns is shown. These test patterns are as follows.

- File formats are Microsoft Word 97, Excel 97, Power Point 97, and so on.
- Characters, graphs, pictures, tables, figures, images, and so on are included.
- Page numbers are from 1 to 12 pages only.
- Both monochrome and color documents are included.

To compare the print-out log size of different logs, the following two kinds of logs were chosen from Table 1.

- Size of spool file
- Size of both thumbnail and text log (shown in Table 2)

5-2. Evaluation result

5-2-1. Size of spool file

The spool-file formats were RAW, EMF, XPS, and PS. The standard-test-patterns were printed-out by a RAW printer driver, an EMF printer driver, a XPS printer driver, and a PS printer driver. Average of their spool-file sizes was then calculated. The calculation results are shown in Fig. 10. The relationship between standard-test-pattern size and average spool-file size is almost proportional. The average spool-file size is as about 1.85 times bigger than that of the standard-test-patterns.

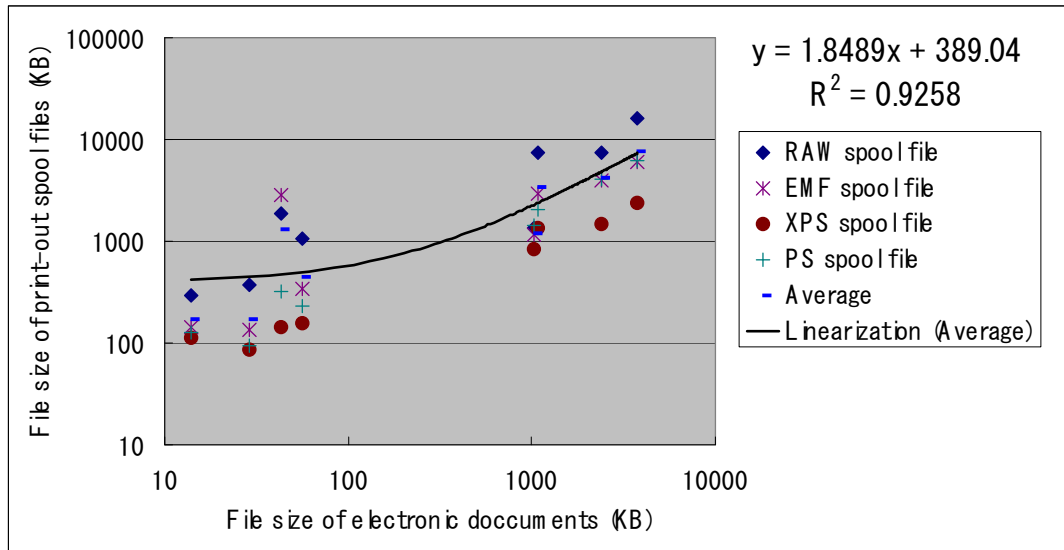


Fig. 10: Average size of spool files (RAW, EMF, XPS, and PS)

5-2-2. Size of thumbnail and text log

Total size of the log is the thumbnail log size plus the text log size. The standard-test-patterns are printed out by the virtual printer driver described in section 4.2. Two kinds of log sizes were then added. The result is shown in Fig. 11. The total size is as about 0.04 times bigger than that of the standard-test-patterns.

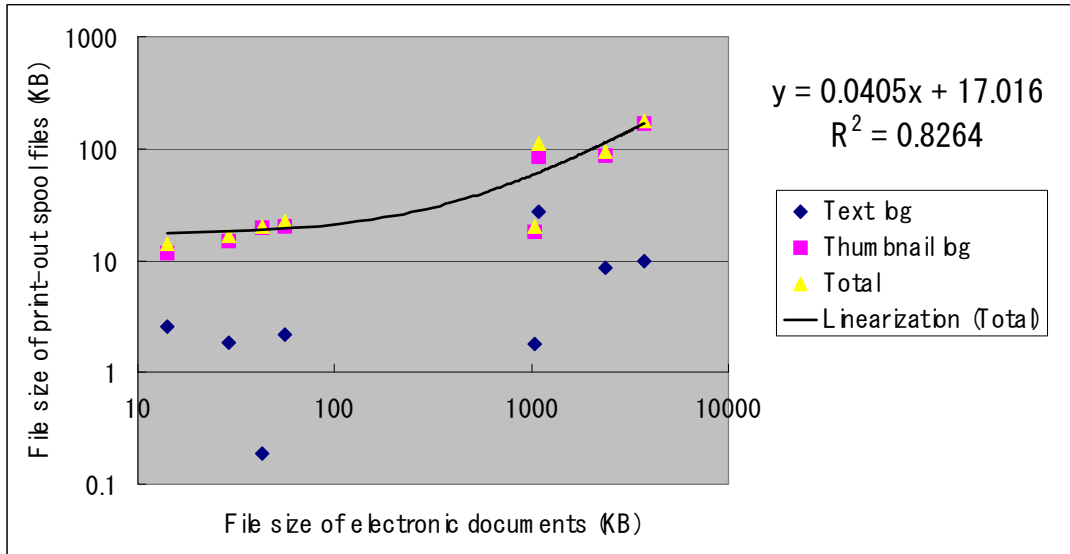


Fig. 11: Total size of thumbnail and Text Logs.

5-3. Application to typical office

The required storage size was estimated for the office supposed as follows.

- 30 employees share 1 printer
- Each employee print outs 3000 pages per year
- Average printed-out electronic document size is 1 MB

If the print-out log is a spool file, the estimated size is 201.4 GB per year. If the print-out log is a thumbnail and text log, the estimated size is 5.2 GB per year. In other words, the thumbnail and text log size decreases by 97.4% compared to the spool file. This means that only 2.6% of the storage space is needed in the case of the thumbnail and text log compared to the spool file.

6. RELATED WORKS

(1) Print-out logs

Related print-out forensic work have been done on print servers (Canon, 2008 [16] and Ricoh, 2008 [17]). The print servers acquire text information from the print jobs and put the print-out records in storage. In another research (Fujii, 2010 [18]) text information is acquired by EMF spool file. This work demonstrated a virtual printer driver that acquires text information. The virtual printer driver is faster in acquiring text information than the work on the print servers.

(2) Watermark print

Watermark print outs have also been researched (Ono, 2004 [19]). A watermark, which includes date, username, and filename, is printed out on paper documents. If a paper document was leaked, the watermark can be extracted by scanning, and the investigator can determine the date, username, and filename. A watermark print is thus useful only after an information leakage; in contrast, the distributed print-out monitoring system developed in the present work is useful not only after a leakage but also for daily control and periodical auditing.

7. CONCLUSION

A distributed print-out monitoring system—composed of a virtual printer driver and a print-out policy/log management server—was developed. The virtual printer driver acquires text information by DDI hooking, performs GREP search to check the content, and creates a thumbnail and text log. The log size is about 0.04 times bigger than as that of printed-out electronic files. That is, compared to the storage size required for retrieving a print-out log as a spool file, the required storage size for the virtual driver is 97.4% smaller. In our future work, we will address the challenge of confirming the actual usefulness of the system for forensic investigation after information leakage.

Windows, Windows XP, Microsoft Word, Excel, and PowerPoint are registered trademarks of Microsoft Corporation in the United States and/or other countries.

Unix is a registered trademark of The Open Group in the United States and other countries.

Mac is a registered trademark of Apple Computer, Inc., in the United States and other countries.

REFERENCES

- [1] Kevin Craine (2000), “Designing a Document Strategy”, MC2 Books.
- [2] NPO Japan Network Security Association (2010), “Year 2009 Research Report about Information Security Incidents Version 1.1” (in Japanese), <http://www.jnsa.org/result/incident/2009.html>, 2011-01 accessed.
- [3] Ikuo Takahashi (2008), “Use of Digital Forensics and the legal problems in information leakage incident response in Japan”, Proceedings of 4th Annual IFIP WG 11.9 International Conference on Digital Forensics - Short Papers -, pp. 65-72.
- [4] Tokyo Metropolitan Police Department (2010), “Report about information leakage incident of international terrorism related data on the Internet” (in Japanese), http://www.keishicho.metro.tokyo.jp/image/jian_101224.pdf, 2011-01 accessed.
- [5] Adobe (2011), “Adobe LiveCycle Rights Management ES2” (in Japanese), <http://www.adobe.com/jp/products/livecycle/rightsmanagement/>, 2011-03 accessed.
- [6] Microsoft (2011), “Information Rights Management” (in Japanese), <http://www.microsoft.com/japan/office/previous/2003/business/irm/default.mspx>, 2011-03 accessed.
- [7] Microsoft (2007), “Log Audit Guide for Microsoft Server Product - Audit for Print Jobs” (in Japanese), <http://technet.microsoft.com/ja-jp/solutionaccelerators/dd285678>, 2011-01 accessed.
- [8] Ricardo Baeza-Yates and Berthier Ribeiro-Neto (1999), “Modern Information Retrieval,” Addison Wesley.
- [9] Microsoft Developer Network (2010), “Rendering a Print Job”, [http://msdn.microsoft.com/en-us/library/ff561943\(VS.85\).aspx](http://msdn.microsoft.com/en-us/library/ff561943(VS.85).aspx), 2011-01 accessed.
- [10] Microsoft Developer Network (2010), “Non-COM-Based DDI Hook-out Functions”, [http://msdn.microsoft.com/en-us/library/ff557586\(VS.85\).aspx](http://msdn.microsoft.com/en-us/library/ff557586(VS.85).aspx), 2011-01 accessed.
- [11] Microsoft (2010), “XPS Specification and License Downloads”, <http://www.microsoft.com/whdc/device/print/xps/downloads.mspx>, 2011-01 accessed.
- [12] Basis Technology (2011), “Rosette Base Linguistics for Japanese” (in Japanese), <http://www.basistech.jp/base-linguistics/japanese/>, 2011-03 accessed.
- [13] Taku Kudo (2009), “MeCab: Yet Another Part-of-Speech and Morphological Analyzer”,

- <http://mecab.sourceforge.net/>, 2011-03 accessed.
- [14] Nara Institute of Science and Technology, Computational Linguistics Lab. (2007), “ChaSen - morphological analyzer”, <http://chasen-legacy.sourceforge.jp/>, 2011-03 accessed.
- [15] Japan Electronics and Information Technology Industries Association (2003), “Standards of Printer Evaluation Pattern”, JEITA IT-3011A.
- [16] Canon (2008), “imageWARE Secure Audit Manager” (in Japanese), <http://cweb.canon.jp/software/output/lineup/secureaudit/index.html>, 2011-01 accessed.
- [17] RICOH (2008), “Ridoc IO Data Selector”, http://www.ricoh.co.jp/IPSiO/related_goods/dataselector/, 2011-01 accessed.
- [18] Yusaku Fujii and Yoshinobu Horita (2010), “Confidential Document Detection by Applying Character Recognition to EMF Print Data”, Proceedings of the Society Conference of IEICE Vol.2010 5, pp. 124.
- [19] Tsukasa Ono and Yuki Egawa (2004), “A Study of Digital Watermark for Printed Image (Security and Society)” (in Japanese), Transactions of Information Processing Society of Japan 45(3), pp. 880-890.