Watermarking Technologies for Security-Enhanced Printed Documents

● Taizo Anan ● Kensuke Kuraki ● Shohei Nakagata

(Manuscript received October 30, 2006)

Sensitive information is not leaked exclusively through computers and networks. In fact, many incidents involve printed documents. It is now possible to protect confidential and private information by applying the following countermeasures when printing documents:
• Copy control by applying a watermark to restrict copying and forgery
• Watermarks for traceability, including background texture watermarks and font embedded watermarks
These two countermeasures can provide total document security by complying with existing security systems and solutions.

1. Introduction

Since April 2005, there have been numerous laws enacted in Japan to protect personal information. The responsibility for protecting this personal information has become a critical issue for enterprise-level businesses. At the same time, the number of incidents involving leaks of personal information is increasing every year. **Table 1** shows the average numbers of victims and estimated claimable amounts for damages in the years 2002 to 2005.

Figure 1 shows that about half of these incidents involve printed documents. This is because conventional security technologies and solutions do not provide sufficient security for printed documents.

Conventional IT security systems have a hierarchical architecture (**Figure 2**). Network security is realized through firewalls and virtual private networks (VPNs), while PC security is provided using such techniques as ciphers and authentication (e.g., passwords, palm vein patterns, fingerprints). Access control is used for e-document security on PCs, server systems, and hardware memory.

However, given the virtual nature of electronic data, these techniques cannot be applied to printed documents. As mentioned above, the new laws protecting personal information combined with an increasing crime rate have created a demand for new technologies intended to eliminate leaks of sensitive information from printed documents.

2. Technologies

To prevent information leaks from printed documents, we have developed the two types of digital watermarking technologies described below.

2.1 Watermarking for copy control

This watermarking technology provides a reminder to deter intentional or accidental unauthorized copying. It embeds into a background texture certain messages that are invisible on original printed documents, but appear clearly on the copies made thereof. It therefore makes people more responsible when handling printed documents, while discouraging the

Table 1
Damages caused by information leaks.

Average number of victims per incident (2002 to 2005)

2002	2003	2004	2005
7,613	30,482	31,057	8,922

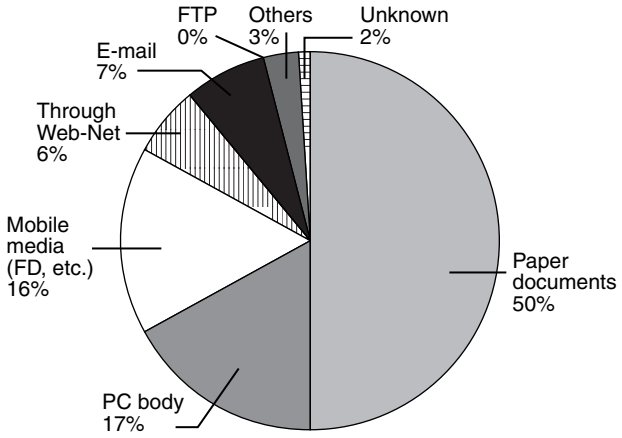
Interannual Changes in Total Projected Compensation for Damages (2002 to 2005)

2002	2003	2004	2005
¥18,922,010,000	¥28,069,360,000	¥466,692,500,000	¥700,178,520,000

Average Projected Compensation for Damages per Incident for 4 years

2002	2003	2004	2005
¥344,040,000	¥550,380,000	¥1,388,970,000	¥708,680,000

Source: NPO Japan Network Security Association: 2005 Information Security Incident Survey Report ver.1.0, table 8, 13, 14, July 31 2006.[1)]
http://www.jnsa.org/result/2005/20060803_pol01/2005incidentsurvey_060731en.pdf



Source: NPO Japan Network Security Association: 2005 Information Security Incident Survey Report ver.1.0, Figure 4, July 31 2006.[1)]
http://www.jnsa.org/result/2005/20060803_pol01/2005incidentsurvey_060731en.pdf

Figure 1
Sources of information leaks.

unauthorized production and circulation of copies. **Figure 3** shows an example of our watermarking for copy control.

The left side of the figure shows an original printed document that includes a watermark, but without the "unauthorized copy" message being visible. However, on the photocopied document on the right side of Figure 3, "unauthorized copy" clearly appears. This is achieved by printing a watermark on an original document using dots and printing smaller dots in the other areas so that both types blend together and appear only as a background texture. The smaller dots are too small to be detected by a photocopier, so when the document is copied, only the larger dots are printed and the watermark becomes visible.

2.2 Watermarking for traceability

This watermarking technology is used for tracing the source of an information leak. It embeds invisible digital data into a printed document, including the name and ID of the person who printed the document, the file name, and the date and time of printing. We have developed two watermarking technologies for traceability: a background texture type and a font embedded type.

2.2.1 Background texture type

This type of watermarking technology embeds identification data into a tint-block background on printed documents (**Figure 4**). Documents containing this type of watermark have a gray tint-block background with what we call a "starlights" pattern. The "stars" are actually holes in the tint-block background, and the positions of these holes indicate the embedded data (**Figure 5**). The complete

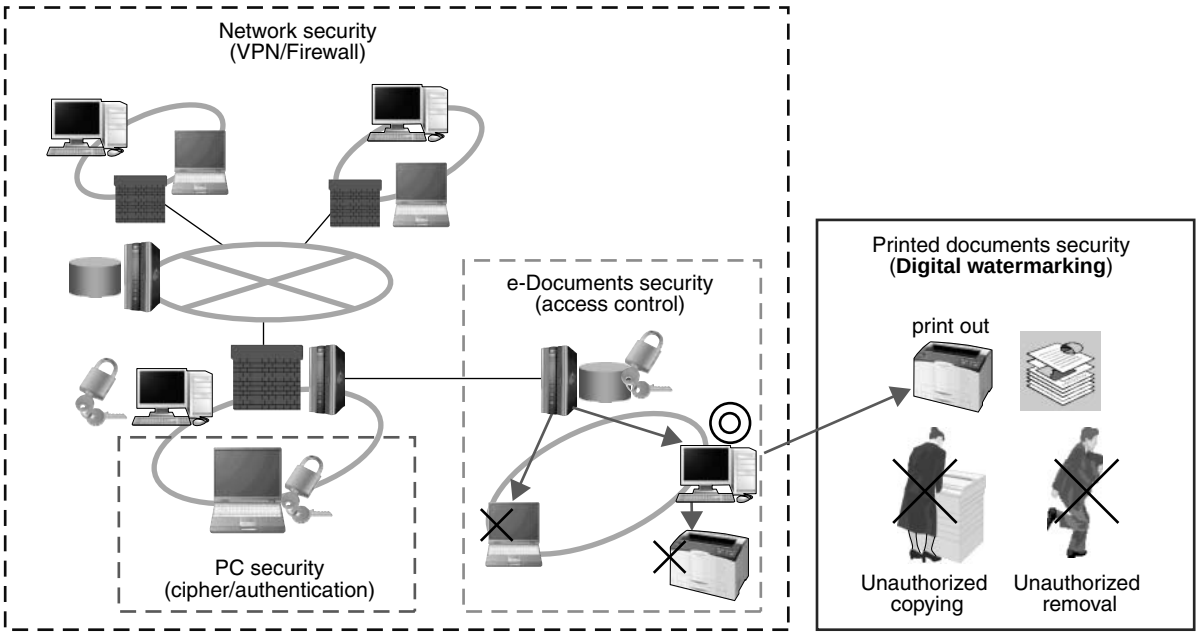


Figure 2
Security hierarchy.

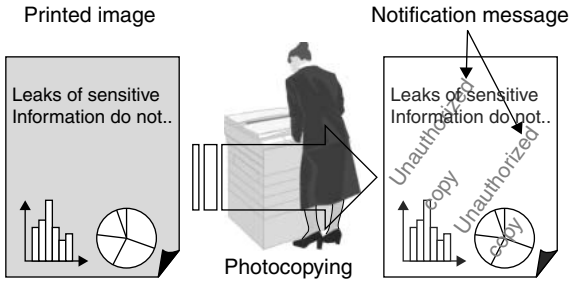


Figure 3
Hidden label that clearly appears on photocopies.

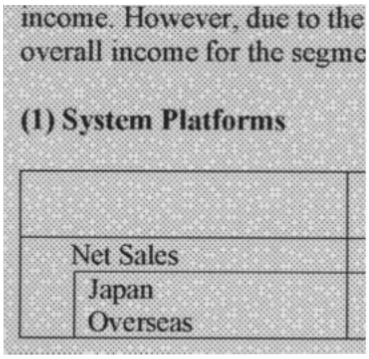


Figure 4
Background texture type watermark.

sequence of holes for the embedded data is repeated over the entire background of the document.

Our starlights pattern has some very important merits for security. One is strong generational copy resistance (with a generational copy being a copy of a copy). Because the starlights pattern is strongly resistant to distortion, rotation, and scaling, it can still be correctly read in a 10th generational copy. Another merit is its high resistance against attempts to decode the embedded data. In Figure 4, we can see that the boundaries between the pattern units are not easy to discern, so it is difficult to know the positions of their holes. This makes it difficult to crack the embedded information.

The main points of our tint-block type watermarks are as follows:

1) Strong generational copy resistance of up to 10 generations
2) Extraction of embedded data even from small portions of a document (For example, 32 bytes can be extracted from a 1/8 portion of an A4 document.)
3) Highly secure pattern unit

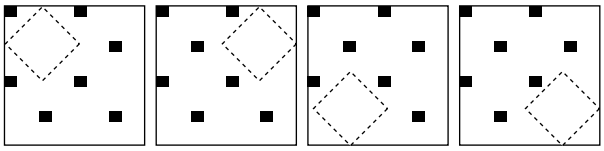


Figure 5
Texture pattern units indicating numbers 0, 1, 2, and 3 from left to right.

2.2.2 Font embedded type

This type of watermarking technology embeds identification data by changing the shapes of printed characters. Documents processed with this technology have no background texture. It can also embed numerical codes into binary images such as font glyphs, figures, drawings, and logos, making it language-independent. Furthermore, it can embed up to 8 bytes of information into a 5 cm^2 area of paper, so even a small portion of a document processed with this technology can be used to identify its source. **Figure 6** shows the results for a portion of a document that was scanned and analyzed by software to extract the watermark. The results are shown at the top left of the figure.

The main points of our font embedded watermarks are as follows:

1) Copy resistance for up to five generations of copies
2) Extraction of embedded data even from small portions of a document (For example, 8 bytes of data can be extracted from a 1/8 portion of an A4 document.)
3) Embedding of data into binary images such as font glyphs, figures, drawings, and logos, making it language-independent

3. Applications

This section describes some example applications of our watermarking technologies for printed documents.

3.1 Copy guard for medical prescriptions

The watermarking for copy control is useful in this case. In the U.S., many crimes are committed involving the illegal acceptance of medicines. Criminals make photocopies of prescriptions and use them to illegally obtain medicines, from which they synthesize narcotics. To prevent this, medical practitioners have requested a copy control system that discriminates between original prescriptions and illegal photocopies. The watermarking is done by client software on the PCs used to print prescriptions, and our watermarking technology can be modified to work with the customer's printer.

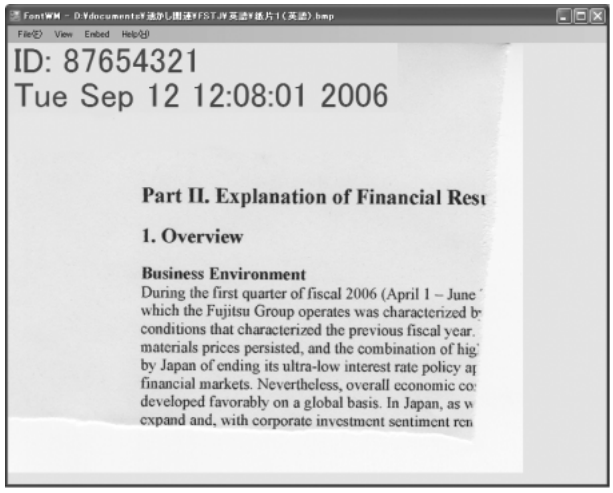


Figure 6
Detecting ID information from a torn piece of document.

3.2 Copy guard for coupons

This is another example of copy control watermarking. Travel agencies issue many coupons for their services, including meal services, optional tour services, and tickets for art museums. Many agencies are concerned about the illegal copying of these coupons because it can cost them a lot of money. Travel agencies currently have two options: they can use special paper that includes a copy control type watermark or buy a special printer that can print a copy control watermark on their coupons. However, both options are expensive.

Our watermarking technology requires no special equipment to provide copy control. The

software for our watermarking technology can be installed on the PC used to print coupons, and costs much less than a special printer or watermark paper.

3.3 Tracing the source of information leaks

The source of information leaks can be traced by using our watermarking for traceability technology. The user installs our watermarking software on a PC used to print documents, and the software embeds information on the documents that indicates the source of the documents and any copies made thereof. Then, if an information leak occurs and a leaked document or one of its copies is obtained as evidence, the source of the leak can be determined.

3.4 Tracing the source of sales on the black market

This is a case similar to the above. Certain products such as drugs are put on the black market, and there is a need to find out where these products are sold and the illegal channels they go through. To do this, a font watermark is embedded into the logos on the packaging boxes of the drugs. The embedded information includes the name of the wholesaler, which helps identify the origin of the drugs.

4. Security system for printed documents

Figure 7 shows how our watermarking technologies can be used to provide security for printed documents. In this example, all client activity is centrally managed on the server, which saves and analyzes the print activity logs and manages the printing policy of each client. The security policy depends on the printer user. For example, if a temporary worker attempts to print out classified documents, the application software on the client PC sends the network server its IP address, the worker's login name, and the time and date when printing was attempted. Then, the server receiv-

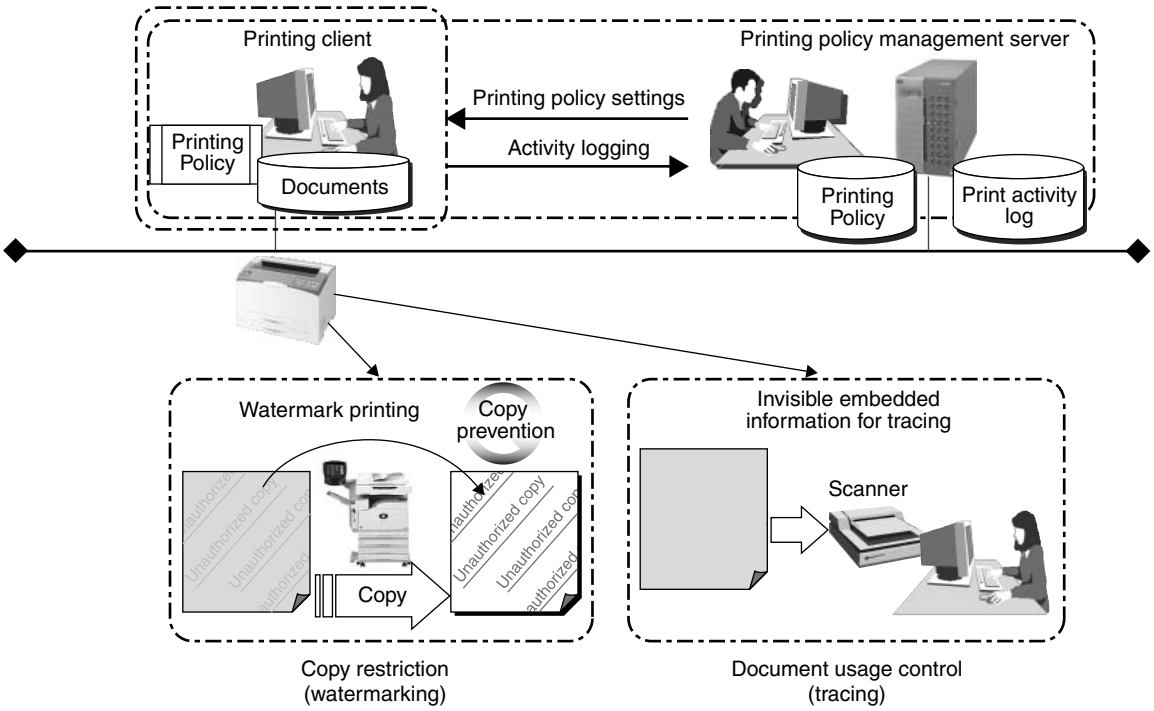


Figure 7
Security system for protecting printed documents.

ing the client's information investigates the security policy and selects which watermarking is appropriate for the client.

If necessary, the server can cancel the watermarking of printed documents for authorized and trusted employees such as senior executives.

Fujitsu Software Technologies has already developed a copy control technology. Moreover, a technology called Paper Tracer is being used in Fujitsu's solutions for printed document security.

5. Conclusion

We have developed two watermarking technologies: watermarking for copy control and watermarking for traceability.

Watermarking for copy control makes it easy to distinguish an original from a copy and is effective in encouraging the careful handling of sensitive and classified documents.

Watermarking for traceability secretly embeds information about the person who prints a document and indicates the source of information. This technology is a strong deterrent against the illegal use of printed documents. We have developed two types of watermarks for traceability: a background tint-block pattern watermark and a font embedded watermark.

These watermarking technologies can be used independently or integrated into an existing office security system to provide new functions for protecting printed materials. Moreover, these technologies can be used to construct a total document security structure that protects against information leaks through E-mail, networks, copying to portable memories, and the theft of printed materials.

Reference

1) NPO Japan Network Security Association: 2005 Information Security Incident Survey Report ver.1.0, July 31 2006. Information Leakage: Projected Damages and Ovsevations (Calculation of Projected Legal Reparations).
http://www.jnsa.org/result/2005/20060803_pol01/2005incidentsurvey_060731en.pdf

Taizo Anan, *Fujitsu Laboratories Ltd.*
Mr. Anan received the B.E. degree in Information Science from University of Tsukuba, Ibaraki, Japan in 1992. He also received the M.E. degree and Ph. D in Engineering from the University of Tsukuba, Ibaraki, Japan in 1994 and 1997, respectively. He joined Fujitsu Laboratories Ltd., Kanagawa, Japan in 1997, where he has been engaged in research and development of algorithms for mobile communication terminals, image processing technologies for high-quality TVs, and digital watermarking technologies for security systems. He is a member of the Institute of Electronics, Information and Communication Engineers (IEICE) of Japan.

Kensuke Kuraki, *Fujitsu Laboratories Ltd.*
Mr. Kuraki received the B.E. and M.E. degrees in Electrical Engineering and Electronics from Aoyama Gakuin University, Tokyo, Japan in 2001 and 2003, respectively. He joined Fujitsu Laboratories Ltd., Kanagawa, Japan in 2003, where he has been engaged in research and development of algorithms for image processing technologies for high-quality TVs, and digital watermarking technologies for security systems. He is a member of the Institute of Electronics, Information and Communication Engineers (IEICE) of Japan and the Institute of Electrical Engineers of Japan (IEEJ).

Shohei Nakagata, *Fujitsu Laboratories Ltd.*
Mr. Nakagata received the B.E. degree in Mathematical Engineering and the M.E. degree in Information Science and Technology from the University of Tokyo, Tokyo, Japan in 2003 and 2005, respectively. He joined Fujitsu Laboratories Ltd., Kanagawa, Japan in 2005, where he has been engaged in research and development of algorithms for image processing technologies for high-quality TVs, and digital watermarking technologies for security systems. He is a member of the Institute of Electrical Engineers of Japan (IEEJ).