Paper Encryption Technology

● Taizo Anan ● Kensuke Kuraki ● Jun Takahashi

(Manuscript received April 6, 2009)

In Japan, since the Act on the Protection of Personal Information was fully enforced in April 2005, companies and other parties have developed various measures to prevent leaks of information. Such measures include preventing information leaks by not printing documents whenever possible, keeping logs of people who print documents, and using electronic watermark technology that can embed tracking information such as IDs in printed material. However, not printing documents may not be possible in some services and may be inconvenient. While electronic watermarks are useful for tracking people who have leaked information, they are not effective for preventing the information leaks themselves. To prevent information leaks while allowing documents to be printed, Fujitsu Laboratories has pioneered a paper encryption technology. With this technology, only those who know the password can access information that is encrypted and hidden in printed material. This report introduces an outline of our paper encryption technology together with its uses and areas of application.

1. Introduction

Even after the Act on the Protection of Personal Information was fully enforced in April 2005, many cases of information leakage have been reported. Among those cases, paper-based media is still listed as the major source of information leakage,[1] and drastic countermeasures are urgently required in this area. As already reported in "Watermark Technology Realizing Security of Printed material,"[2] featured here in May 2007, Fujitsu Laboratories is making continuous efforts to conduct R&D on security technologies for printed materials. However, while electronic watermark technology allows the violator to be tracked after information has been leaked, or raises the alarm immediately before information is leaked, it does not actually prevent the leakage of information itself.

To overcome these limitations, Fujitsu Laboratories has pioneered technology to enable printed material to be encrypted and decrypted in a way similar to that used for electronic data. By using this technology, unauthorized people who do not know the password will not be able to read the information contained in an encrypted document, even if that document is taken out of a controlled area. Accordingly, unlike retrospective countermeasures such as electronic watermarks which are based on tracking the violator after the information has been leaked, it is possible to take preventive measures before the leak actually happens. This technology enhances the security of documents that have been printed and makes possible new services and solutions for preventing information from being leaked from printed material.

2. Outline of encryption and decryption technologies for printed material

2.1 Encryption and decryption processes

As shown in **Figure 1**, this innovative technology encrypts electronic data (for example, an image created by certain word processing software or captured by a digital camera) and printed material. The electronic data are once converted into an image with software called a "virtual printer driver" before being encrypted. The printed material needs to be scanned with a scanner and converted into image data on a computer. Then, the encryption software starts up and encrypts the electronic data and printed material which have been converted into image data. In this encryption process, the user selects the information to be hidden with a mouse or similar device. Then, the user enters a password to start the encryption. The image data that has been encrypted may be converted and saved as electronic data again or printed. The encrypted data can be delivered to the recipient by post, fax or by attaching it to an E-mail. The recipient opens the encrypted data with the software on his or her computer (or scans the printed material with a scanner), and then decrypts it with the software. The data can only be decrypted by those who know the password that was set at the encryption stage.

Package software called DocEncrypt can process data as indicated in Figure 1. It is marketed by PFU Limited.

2.2 Technical challenges

It is impossible to decrypt material that has been encrypted with an existing encryption method after it has been printed out. If a printed material is printed and then scanned, the scanned image data will not be the same as the original image data of the printed material. The coloring and contours of the letters will be significantly

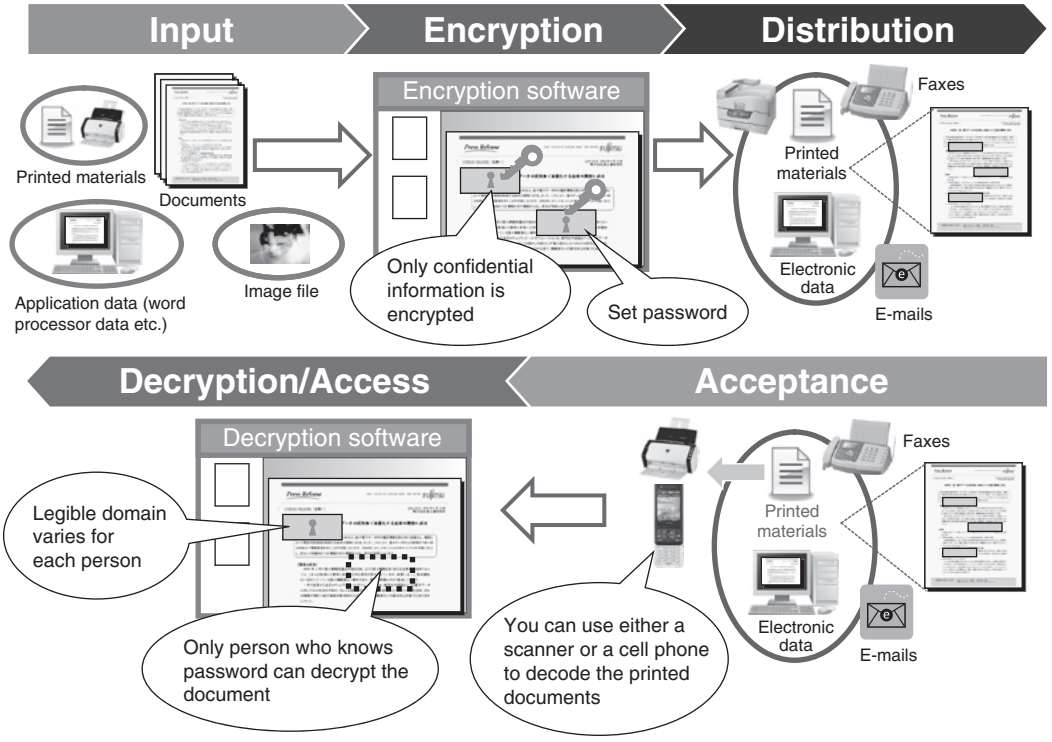


Figure 1
Encryption and decryption process.

degraded compared to those before printing. Existing encryption methods are applicable only to electronic data, and therefore only electronic data that has been encrypted but not been processed in any other way can be decrypted. If the data undergoes any process that degrades it, such as being printed or scanned, it will become impossible to decrypt it, even if it is returned to the format of electronic data.

In order to encrypt printed material in a practical way during everyday business practices, we need to assume that such data will undergo various types of degradation, including the following:

1) Degradation by printing

When a color image is printed, generally the printer will print the image using three or four colors of inks in various densities instead of mixing inks based on the color of the original image. The printed image looks like the original image to the human eye, however, the printed image is actually printed in a quite different manner compared to the original image. People are not aware that the data has been degraded at this stage. Besides, factors such as ink bleeding, irregularities, defects and minor degrees of expansion and shrinking are involved.

2) Degradation by scanning

Degradation occurs when printed material is scanned by a scanner. Shadows, yellowing and darkening may occur even when white paper is scanned. Further, if the resolution of the scanner is poor, the scanner will not scan the original printed matter accurately, leading to noise and blurring. Distortions or tilting during scanning will also affect the quality of the scanned image.

3) Degradation by fax transmission and duplication

The encrypted printed material may also be sent by fax or be duplicated.

Because the scanning resolution of a facsimile machine is lower than that of a scanner, the quality of the faxed material data is degraded. Moreover, since the material data are scanned on a gray scale and then converted into black-and-white images to transmit the data, image degradation associated with conversion errors cannot be avoided.

All the above-mentioned challenges need to be overcome to decrypt and view encrypted documents that have been printed. There is a need for a technical innovation based on an entirely new standpoint.

2.3 Paper encryption technology

To encrypt and decrypt printed material, we have developed the technology from the following standpoints:

1) Method using ambiguity of human sight

Since printers print images in a way that is generally acceptable considering the way human eyes perceive things, the decryption process can use this mechanism too. Namely, instead of adopting the existing encryption system where even a single bit of change in data prevents the information from being decrypted, we propose a system that allows data to be decrypted even if it has undergone a slight change that is imperceptible to human eyes.

2) Method unaffected by distortions, tilting, expansion and shrinkage

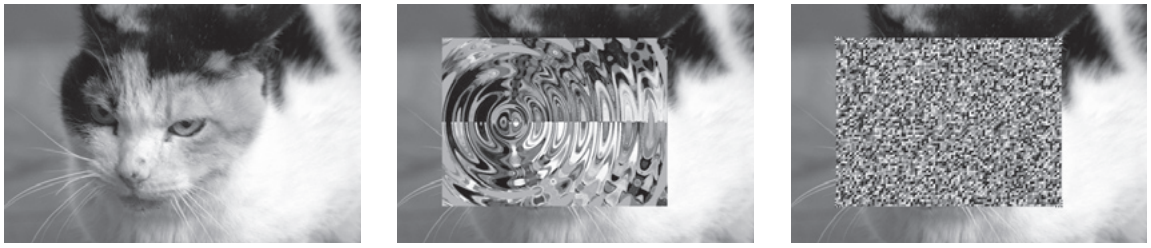
We need a method that decrypts scanned data even if the image data have been distorted, tilted, expanded or shrunk when scanned.

3) Possibility of use as electronic data

By assuming the situation where encrypted data are used as electronic data without being printed, we propose a method that allows such data to be completely converted into the original data when they are decrypted, similar to a method supported by conventional methods.

Our innovative paper encryption technology reflects all of the above-mentioned considerations.

Figure 2 shows an outline of our encryption method. The encryption of image data is based on scrambling (strictly speaking, scrambling does not mean encrypting; however, for the purposes



(a) Original image (b) Conversion of image (c) Encrypted image

Figure 2
Overview of our paper encryption technology.

of this report we shall assume that scrambling means hiding information, which is roughly equivalent to encryption). Because scrambling is a process that divides an image into many small patches and then changes the position of individual patches, we need to satisfy the requirement stated in 1) above. To be specific, an insignificant level of degradation associated with printing and scanning may be neglected because such changes are imperceptible to human sight. However, because scrambling guarantees only a low level of security, our method inserts a special image conversion process before the scrambling process. Through this conversion, it is impossible to obtain the original image even if a violator makes a magnified copy of the encrypted document, cuts it into pieces with scissors and then reassembles it like a jigsaw puzzle.

Encrypted data can be decrypted by finding out the encrypted domains from the scanned image data with the software and then conducting the encryption process in reverse. Because the user will know in advance the specific geometry of the small patches created by the scrambling, for example they might be rectangular or triangular, it is possible to correct the distortion for each patch. In this way, the user can reproduce even small letters (e.g. 8 pt.) by decryption.

2.4 Using cell phones with paper-based encryption

When considering the use of a scanner for decrypting printed material, we mainly assume

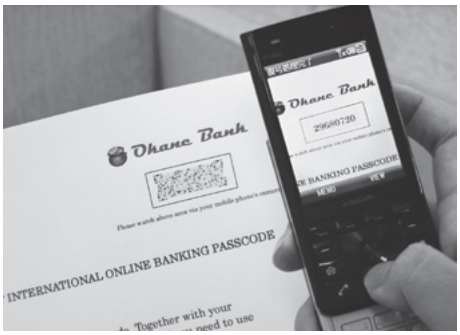


Figure 3
Decryption with a cell phone.

the situation where bulk processing is conducted, in which a large amount of encrypted printed material is decrypted in one go. However, cell phones are easier and more convenient tools to use than scanners when people want to immediately read a small document or transmitted fax. Along with the development of a decryption method using scanners, Fujitsu Laboratories has developed a method to decrypt data contained in printed material by using cell phones equipped with a camera feature (**Figure 3**). In addition to the technical requirements for decrypting data using scanners, the following issues need to be addressed when using a cell phone with a camera feature as a decryption tool.

1) 3D distortion

When using a cell phone for decrypting data, several factors that do not come into play when decrypting with a scanner need to be considered, including the distance between the camera and the object, the tilting angle of the camera, and

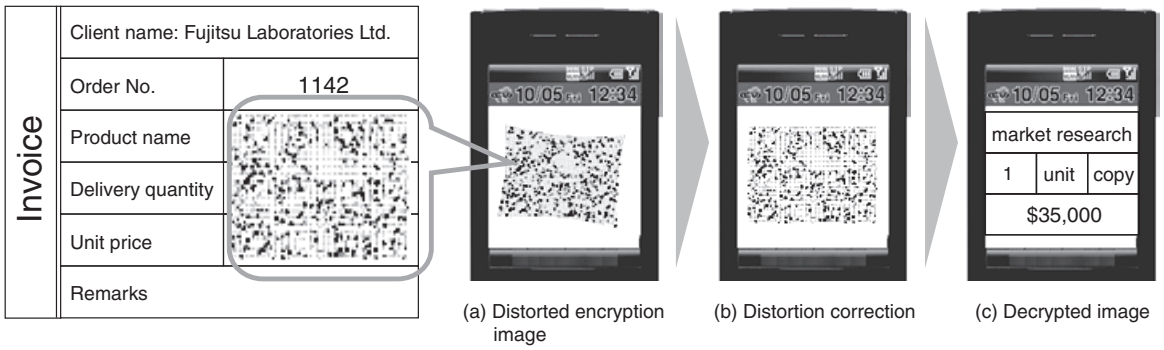


Figure 4
Distortion correction.

the distortion associated with lens. **Figure 4** indicates how distortion of the captured image is corrected and how it undergoes decryption processing. Figure 4 (a) shows an image captured in a distorted manner, while Figure 4 (b) shows the same image after it has been corrected and Figure 4 (c) shows the image after it has been decrypted.

2) Optical noise

It is necessary to assume the situation where users carry out decryption processing in an indoor environment where the amount of illumination changes frequently or under sunlight. Because of shadows that may be cast on the printed material, there will be bright sections and dark sections generated in an encryption domain, which makes decryption difficult because there is an increased tendency for degradation. **Figure 5 (a)** shows an image that has been captured while a shadow was cast over it. If this image is decrypted without being corrected, texture-like noise will be generated in the background because of reverse scrambling, where dark sections and bright sections are scattered in small pieces as shown in **Figure 5 (b)**. On the other hand, **Figure 5 (c)** shows the image after it has undergone brightness correction and optical noise has been removed. The decrypted image has uniform brightness and also the text is more legible because there is enhanced contrast with the background.

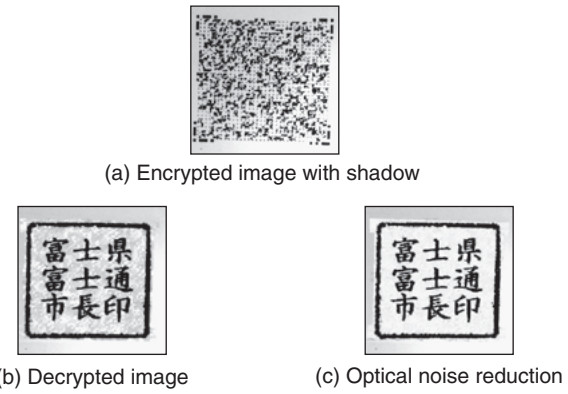


Figure 5
Optical noise reduction.

3) Blurring

Users sometimes read printed material by holding it with one hand while holding their cell phone in the other hand. In addition, printed material is decrypted in our cell phone system by using the cell phone camera's close-up feature. These facts tend to lead to serious image quality degradation due to blurring. Therefore, as shown in **Figure 6**, we inserted an additional process before decryption, where the cell phone's processor judges whether or not the obtained image has been blurred using simple, high-speed blur detection processing. If the cell phone processor judges that the image has been blurred, it disposes of the image without sending it to the next decryption processing and starts checking the next image. In this way, the quality of the image to be decrypted is improved via this repetitive checking process so that a non-blurred

image is selected.

We managed to overcome these technical challenges specific to a cell phone environment and successfully decrypted some encrypted printed material using a cell phone based on the above-mentioned approaches. In addition, we have discovered that if the resolution of the camera is increased, a better image quality can be obtained after decryption. However, because this increase of resolution will lead to a longer processing time, we need to speed up the processing.

3. Uses and applications

We think there will be a number of uses and applications for our encryption technology for printed material.

3.1 Uses

1) Document security during storage and transportation out of controlled areas

Because printed material can be encrypted, it is possible to encrypt all documents that should be printed and stored in a controlled area, documents that are taken out of that controlled area, and even data stored in notebooks. This makes it possible to protect confidential information on all paper-based media. Because confidential documents in briefcases are lost or stolen very often, there are needs to use such preventive measures to prevent information leaks.

2) Protection of fax transmissions

Information is still sometimes leaked when data is sent by fax. Currently, many documents such as purchase orders, acceptance receipts, financial records and customers' application forms are transmitted via facsimile. Actually, some companies stipulate that more than one staff member should be present when faxes are being sent to prevent erroneous transmission. However, even if the sender carefully checks the recipient's fax number, information may still be leaked if that recipient has changed his or her fax number without telling the sender. If our technology is applied, the sender can hide the data to be transmitted. Only those who have a way to decrypt the data (have the software) and know the password are able to decrypt the data, so information leaks caused by erroneous fax transmission can be prevented.

3) Tamper-detection of printed material

As shown in **Figure 7**, certain information that needs to be protected from tampering is printed twice, and one of the sheets has been encrypted. Even if a violator tampers with the unencrypted information, he or she will not be able to tamper with the other (encrypted) information in exactly the same way. Therefore, by decrypting the encrypted information and comparing it with the exposed information, it is possible to find out whether or not the

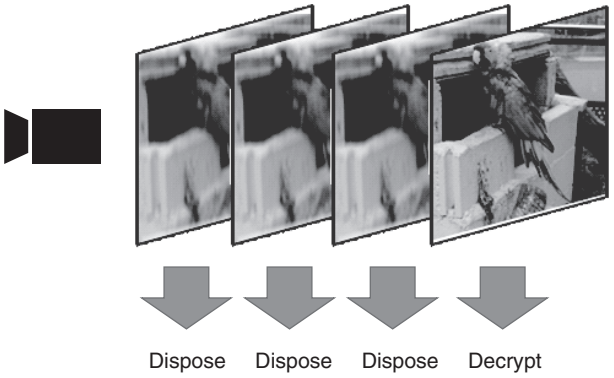


Figure 6
Blur reduction by selecting image.

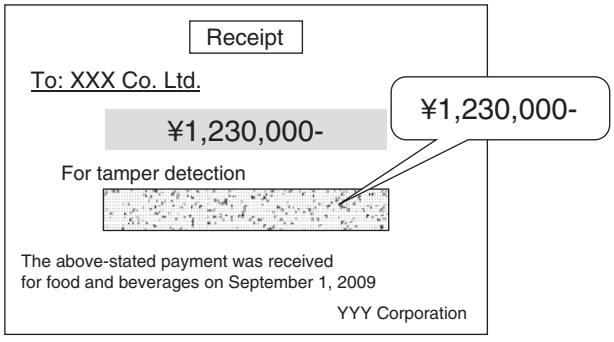


Figure 7
Tamper-detection with our paper encryption technology.

information has been tampered with. Because the password is confidential, the violator cannot tamper with the data even if he or she has the encryption software.

3.2 Example of applications

There are several applications for our paper encryption technology.

1) Avoiding preparation of the same document twice through partial encryption

Some types of documents such as fault control sheets, corporate governance and internal audit data, evaluations of company operations, design specifications and court disclosure documents need to be prepared anew before being submitted. If the original version includes information that should be kept confidential while the rest of the information in the document needs to be made public or shared with a third party, the current practice is to prepare a new version excluding the confidential information or to apply a black mark covering up the confidential information. However, by using our technology, the original copy can be partially encrypted and the time spent on preparing a new version can be saved. Because only those who know the password can decrypt the information, there is no need to produce the document twice.

2) Reducing labor of hiding confidential information in documents with a black mark

When documents that include confidential information such as a customer questionnaire are shared among multiple sections of a company, encryption technology can be used appropriately so that only the age, gender and requests of the customers for products are disclosed to the marketing division, while only their requests are disclosed to the sales outlets. On the other hand, the staff in the customer claim center who directly interact with the customers will need to be able to decrypt all the information. In this way, our technology can offer wide-ranging access control for information. A secondary benefit of our encryption technology is that it reduces the amount of carbon copy paper used. Multi-sheet documents such as customer application forms often include carbon copy paper to duplicate information on each sheet. However, because our paper encryption technology offers an alternative way to do this with a single sheet, there is no need to use carbon copy paper, resulting in cost reduction.

3) Outsourcing of services including confidential information

It is difficult to completely outsource services in which confidential information is handled from the standpoint of preventing information leaks. However, by using our paper encryption technology, it is possible to disclose the minimum amount of information necessary to the external party. For instance, in the example of a simple service such as entering confidential information on a computer system, the following workflow is often used: Data entry is performed by a contractor company that accesses the server of the client company from its computers. If the client discloses only some of the names, addresses and telephone numbers in the list to Contractor A and the remaining names, addresses and telephone numbers to Contractor B for data entry, the confidential information can be protected, unless Contractor A and Contractor B cooperate with each other to elicit the hidden information.

4. Future developments

We are reviewing the feasibility of encrypting printed material in SaaS format. With this system, decryption is carried out also in SaaS format or by using a cell phone with a camera feature. This makes it possible for users to use updated services on a continuous basis without installing special software on their computers or maintaining such services by themselves. In an organization requiring a higher level of security, keys can be distributed automatically and safe services offered that are linked with personal authorization for the decrypting person.

5. Conclusion

This report described some paper encryption technology pioneered by Fujitsu Laboratories, as a world-first approach, together with its uses and applications. By encrypting printed material, it is possible to prevent information from being leaked when printed material is taken out from a controlled area or when a fax is erroneously sent. Some organizations favoring the convenience of printed material will hesitate to implement security countermeasures if they find it inconvenient to do so. However, statistics on the sources of information leaks indicate that paper-based media is the largest source (55%). Customers' confidential information that is held by an organization is continuously at risk unless such organization implements appropriate countermeasures as soon as possible. Because our paper encryption technology makes it possible to promptly access an encrypted domain with a cell phone, a tool widely used by the general public, the convenience of paper-based media is maintained while ensuring security. We plan to further improve the convenience of our technology in future by reflecting in it the opinions of the users and customers who have shared their confidential information with external organizations.

References

1) NPO Japan Network Security Association: FY2008 Investigation Report on Information Security Incidents (Ver.1.3). (in Japanese). *http://www.jnsa.org/result/2008/surv/incident/2008incident_sruvey_v1.3.pdf*
2) Taizo Anan et al.: Watermark Technology Realizing Security of Printed material. (in Japanese), *FUJITSU*, Vol. 58, No. 3, pp. 183–187 (2007).

Taizo Anan
Fujitsu Laboratories Ltd.
Dr. Anan received a B.E. degree in Information Science from the University of Tsukuba, Ibaraki, Japan in 1992. He also received an M.E. degree and a 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, digital watermark technologies for security systems, and the paper encryption technology. He is a member of the Institute of Electronics, Information and Communication Engineers (IEICE) of Japan.

Kensuke Kuraki
Fujitsu Laboratories Ltd.
Mr. Kuraki received 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, digital watermark technologies for security systems, and the paper encryption technology. 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).

Jun Takahashi
Fujitsu Laboratories Ltd.
Dr. Takahashi received B.E. and M.E. degrees in Information Systems Engineering and a Ph. D. degree in Information Networking from Osaka University, Osaka, Japan in 2001, 2003 and 2006, respectively. He joined Fujitsu Laboratories Ltd., Kanagawa, Japan in 2006, where he has been engaged in research and development of digital watermark technologies for security systems, and the paper encryption technology. He is a member of the Institute of Electronics, Information and Communication Engineers (IEICE) of Japan.