A Study on Data Management Using Mobile Computing With Digital Watermark Technology

Manabu Hirakawa, Junichi Iijima

Department of Industrial Engineering and Management, Graduate School of Decision Science and Technology, Tokyo Institute of Technology
1. Introduction
2. Basic Technology of Digital Watermarking
3. Comparison with Existing Technologies
4. Applications in Information Management
5. Conclusion and Future Work
Background of Research

Characteristic of Digital Content
Quality does not deteriorate even if the content is duplicated
color to be handled.
easily duplicated illegally.

With the advent of digital technology, problems involving digital content, such as media piracy and copyright infringement, have come into the open.

This paper focuses on the relation between data management and strong security, and considers a management method which uses digital watermarking technology.
Problems

1. Loss of confidence in information management
   Current management methods are built on the assumption that there is no problem with the people involved in information management activities.

2. Determining the particulars of distribution routes
   There is no authentication capability in the products that are being distributed.

3. Increase in information management costs
   The cost of information management becomes a burden and is reflected in product costs.
Objective for Solutions

In order to assure safety, technology that assures strong security and makes it impossible for third parties to alter information is necessary.

Digital watermarking will be used as the solution

1. High reliability
2. Strong security
3. Low cost

DPM: Direct Parts Marking
About Digital Watermarking

The information is embedded in the contents

Detecting the information from the contents
In addition to color processing, grayscale processing is also possible.

- Image data is rewritten at the pixel level, and the desired information is embedded. Information for the image is formed over a fixed area.

- Accuracy of the information is improved by cross-checking across multiple tiles when detecting.

- In addition to color processing, grayscale processing is also possible.
Aspects of Comparison

A new technique often introduced in distribution management uses QR codes and RFIDs. Here, we have compared digital watermarking technology with QR codes and RFIDs.

- **Reliability, ease of mounting**
  - heat resistance, water resistance, minimum required area, degree of freedom of the shape

- **Security Considerations**
  - Confidentiality, obfuscation against duplication, obfuscation against alteration

- **Cost**
  - Supports read input devices
- With RFID, RF tags have the possibility of being destroyed by heat (one-chip IC element).
- With QR codes there is a problem in that the item to be managed is marked, and there is a problem in maintaining the state of the print copy.
- QR codes have a problem with the degree of freedom of the shape and security.
- With RFID, the cost of RF tags becomes a problem because of the massive quantity of managed objects.
- Digital watermarking is supported by few read devices, and is not common at the present stage.

### Technology Comparison

<table>
<thead>
<tr>
<th>Characteristic</th>
<th>Comparison items</th>
<th>Digital watermarks</th>
<th>QR codes</th>
<th>RFID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Heat resistance</td>
<td></td>
<td>○</td>
<td>△</td>
<td>×</td>
</tr>
<tr>
<td>Water resistance</td>
<td></td>
<td>○</td>
<td>△</td>
<td>×</td>
</tr>
<tr>
<td>Minimum required area</td>
<td></td>
<td>○</td>
<td>×</td>
<td>△</td>
</tr>
<tr>
<td>Degree of freedom of shape</td>
<td></td>
<td>○</td>
<td>×</td>
<td>△</td>
</tr>
<tr>
<td>Confidentiality</td>
<td></td>
<td>○</td>
<td>×</td>
<td>△</td>
</tr>
<tr>
<td>Obfuscation against duplication</td>
<td></td>
<td>○</td>
<td>×</td>
<td>○</td>
</tr>
<tr>
<td>Obfuscation against alteration</td>
<td></td>
<td>○</td>
<td>×</td>
<td>○</td>
</tr>
<tr>
<td>Ease of reading</td>
<td></td>
<td>△</td>
<td>△</td>
<td>○</td>
</tr>
<tr>
<td>Cost</td>
<td></td>
<td>○</td>
<td>○</td>
<td>×</td>
</tr>
<tr>
<td>Compatibility with read devices</td>
<td></td>
<td>△</td>
<td>○</td>
<td>○</td>
</tr>
</tbody>
</table>

(○: Applicable  △: Partially applicable  ×: Not applicable)
Examples of Direct Parts Marking

- **Metals**
  - Printed circuit boards
  - Acrylic board
  - Fabric

- **Visible**
- **Invisible**
By applying digital watermarking technology to brand-name merchandise designs, the legitimacy of the product can be proven, and the product route from the place of origin can be identified. A link to the relevant brand’s website can also be added.
Determining vehicle models

Apply digital watermarking technology to car coating and parts means the car's unique data can be used as a theft detection and crime-prevention measure.

Also, services could be provided such as promotions with information about new car models from the car manufacturer, or the current market price for used cars.

As theft-detection or crime-prevention technology.
Confirm recalled parts.
Check product information when purchasing a used car, etc.
Solution for Problems

Conditions not met by existing recognition technologies (2-dimensional barcodes and RFID)

- Susceptible to heat and dirt
- Shape (small, curved) does not match
- Cannot withstand long-term usage

Solution to the above problems

→ Digital watermarking and Direct Parts Marking

- High heat and water resistance
- Entire material can be processed
- Not dependent on size or shape
- Appropriate for long-term usage
- Bonus: Authenticity determination and forgery prevention
Digital watermarking technology is growing as an essential technology for promoting the sound distribution of digital contents. In future, we will see digital watermarking technology as a factor in mobile business models that develop through services.
Future Works

1) Categorization of service models for service configurations that will be used.

2) Construction of a system model that allows for sound operation.

3) Attack resistance verification.
Thank you for your kind attention.